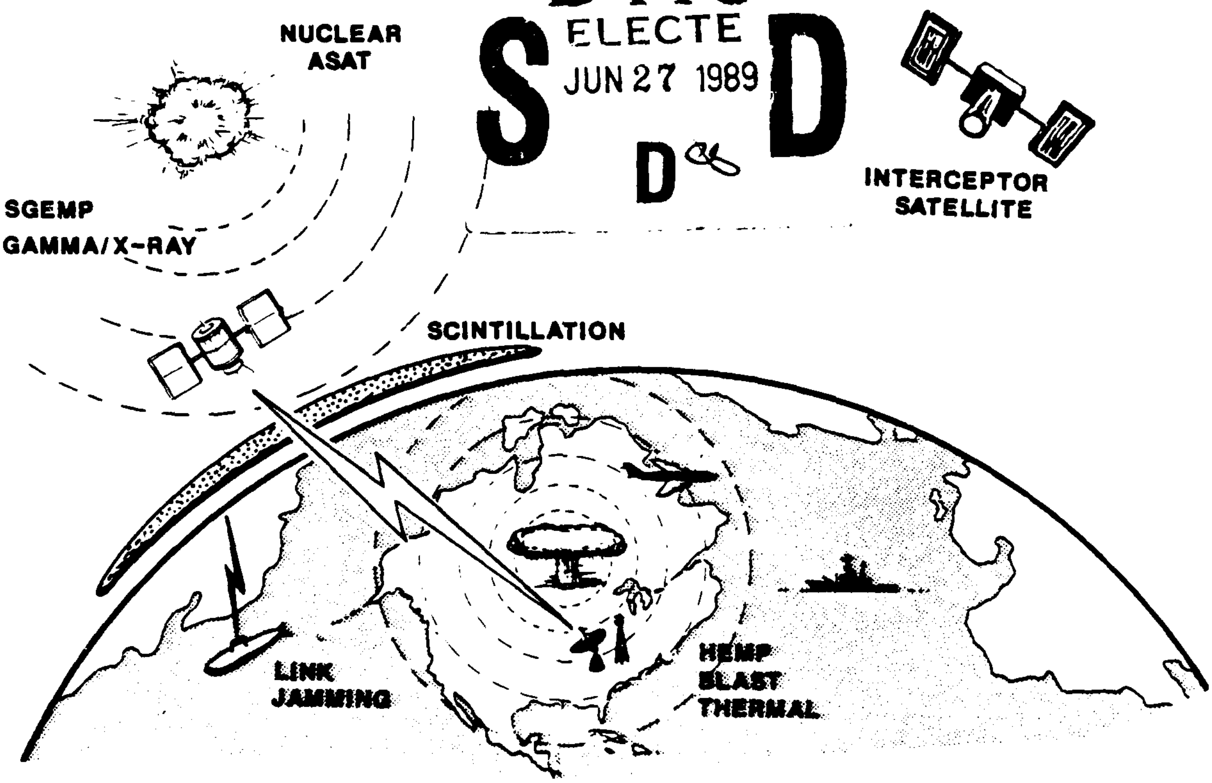
DIRECTORATE OF ANALYSIS

AIR FORCE OPERATIONAL
TEST AND EVALUATION CENTER
KIRTLAND AIR FORCE BASE
NEW MEXICO 87117-7001

DEVELOPING OPERATIONAL THREAT SCENARIOS



TECHNICAL PAPER 11.0 APRIL 87 OPR: AFOTEC/OAS

PREFACE TO THE ANALYSIS DIRECTORATE

TECHNICAL PAPER SERIES

These technical papers are not intended to set AFOTEC or OA policy about their subject matter. They are not directive, but informative. This series was begun to provide analysts with technically adequate starting points for their individual programs. Use them as they were intended: hands-on reference works.

Donald M. Douglas

Donald M. Douglas, Col, USAF
Director of Analysis

This series of technical papers will only be as good as you, the ops effectiveness analysts, make it. Certainly each paper can be improved, and there may be additional subject areas of general interest. I solicit your feedback and constructive criticism. All the papers can be rapidly edited and redistributed, so if you have thoughts please contact me.

Mike Stolle

Mike Stolle, GM-15
OA Technical Advisor

TABLE OF CONTENTS

LIST OF FIGURES
LIST OF ACRONYMS

SECTION		PAGE
1.0	INTRODUCTION	1
	1.1 PURPOSE OF OPERATIONAL SCENARIOS	2
	1.2 GENERAL DIRECTIONS FOR SCENARIO DEVELOPMENT	3
	1.3 OVERVIEW OF SCENARIO DEVELOPMENT PROCESS	5
	1.4 MOBILE C^3 EXAMPLE OF OPERATIONAL SCENARIO	7
	1.5 ORGANIZATION OF THE DOCUMENT	10
2.0	SYSTEM MISSION DESCRIPTION	12
	2.1 INTRODUCTION	12
	2.2 DATA SOURCES	13
	2.3 MISSION ATTRIBUTES	13
	2.4 SYSTEM ATTRIBUTES	14
	2.5 MISSION DESCRIPTION PROCEDURE	15
	2.6 EXAMPLE MISSION DESCRIPTION	20
3.0	THREAT DESCRIPTION	24
	3.1 INTRODUCTION	24
	3.2 DATA SOURCES	25
	3.3 PRINCIPLES	30
	3.4 NUCLEAR THREATS	34
	3.5 CONVENTIONAL THREATS	37
	3.6 ELECTRONIC WARFARE THREATS	38
	3.7 CHEMICAL/BIOLOGICAL THREATS	40
	3.8 DIRECTED ENERGY WEAPONS	41
	3.9 TYPICAL THREAT TREES	42
	3.9.1 ICBM System	42
	3.9.2 Strategic Aircraft System	44
	3.9.3 C^3 System	44
	3.10 THREAT DESCRIPTION FOR SLINK SYSTEM	44
4.0	DEVELOPING AND REFINING THE OPERATIONAL SCENARIO	51
	4.1 INTRODUCTION	51
	4.2 DATA SOURCES	52
	4.3 GENERAL PRINCIPLES	53
	4.4 INITIAL APPLICATION	55
	4.5 REFINING THE SCENARIO	57
	4.5.1 Susceptibility Analysis	59
	4.5.2 Vulnerability Analysis	60
	4.5.3 Prioritized Mission/Threat Interactions	62
	4.6 ADDITIONAL CONSIDERATIONS	63
	4.7 CONCLUSION OF MOBILE C^3 EXAMPLE	65

TABLE OF CONTENTS (Continued)

SECTION		PAGE
5.0	SUMMARY: INTEGRATING THE SCENARIO INTO THE OT&E	70
5.1	OVERVIEW	70
5.2	USING COMMANDS AND STUDIES AGENCIES	70
5.3	OTHER SYSTEM OT&E TESTING	71
5.4	JOINT OT&E/DT&E	71
5.5	SUMMARY	72

REFERENCES

APPENDIX A: Index to Air Force Nuclear Survivability Data Base

APPENDIX B: OT&E Plan Supplement B (Operational Threat Scenario)-Sample Annotated Outline

LIST OF FIGURES

FIGURE		PAGE
1-1	SATCOM Operational Scenario	1
1-2	Scenario Development Flow Diagram	6
1-3	SLINK System	8
1-4	Operational Scenario for SLINK C^3 System	9
2-1	Operational Scenario Development Process (Mission Description)	12
2-2	Typical Bomber Mission Profile	17
2-3	Typical Bomber Missions Functions vs. Mission Phase	19
2-4	SLINK C^3 Mission Timeline	21
3-1	Operational Scenario Development Process (Threat Description)	24
3-2	ICBM Threat Description	26
3-3	Survivability Elements	32
3-4	Summary of Nuclear Weapons Environments	36
3-5	Threat Tree for ICBMs	43
3-6	Threat Tree for Strategic Bomber	45
3-7	Threat Tree for C^3 System	46
3-8	Threat Description for SLINK System	47
3-9	SLINK Threat Description Table	49
4-1	Operational Scenario Development Process (Refinement)	51
4-2	Initial Application of Threat to Strategic Bomber (Matrix)	56
4-3	Initial Application of Threat to Bomber Timeline	58
4-4	Prioritizing Threat/System Interaction (Strategic Bomber)	64

LIST OF FIGURES (Continued)

FIGURE		PAGE
4-5	SLINK Operational Scenario Outline	66
4-6	SLINK Operational Scenario Refinement	68

LIST OF ACRONYMS

AAM	Air to Air Missile
AFCC	Air Force Communications Command
AFCSA	Air Force Center for Studies & Analysis
AFEWC	Air Force Electronic Warfare Center
AFM	Air Force Manual
AFSC	Air Force Systems Command
AFWL	Air Force Weapons Laboratory
AI	Airborne Intercepter
ASAT	Anti-Satellite (Weapon)
ASM	Advanced Strategic Missile
BIT	Built-In Test
C^3	Command Control and Communications
C^3CM	C^3 Countermeasures
CEP	Circular Error Probable
COMINT	Communications Intelligence
COMM	Communications
CONUS	Continental United States
CONV	Conventional
DCP	Decision Coordinating Paper
DEMP	Dispersed EMP
DEW	Directed Energy Weapons
DF	Direction Finding
DIA	Defense Intelligence Agency
DT&E	Development Test and Evaluation
EAM	Emergency Action Message
ECCM	Electronic Counter-Countermeasures
ECM	Electronic Countermeasures
EHF	Extremely High Frequency
ELINT	Electronic Intelligence
EMP	Electromagnetic Pulse
EOCM	Electro-optical Countermeasures
ESC	Electronic Security Command
ESM	Electronic Support Measures
FM	Field Manual
FMECA	Failure Mode Effects and Criticality Analysis
HE	High Explosive
HEMP	High Altitude EMP
HF	High Frequency
HPM	High Power Microwave
HQ	Headquarters
ICBM	Intercontinental Ballistic Missile
INS	Inertial Navigation System
IOT&E	Initial Operational Test & Evaluation
IRBM	Intermediate Range Ballistic Missile
IR	Infra-Red

JCM	Joint Chiefs-of-Staff Manual
JMSNS	Justification for Major System New Start
JX	Jamming
LORAN	Long Range Navigation
MAJCOM	Major Command
MCF	Mission Critical Function
MESL	Mission Essential Subsystems List
MIA	Missile Intelligence Agency
NATO	North Atlantic Treaty Organization
NBC	Nuclear Biological Chemical
NCGS	Nuclear Criteria Group Secretariat
NIS	Naval Intelligence Service
NMC	Non Mission Capable
NSA	National Security Agency
OT&E	Operational Test and Evaluation
PACAF	Pacific Air Forces
PE	Program Element
PMC	Partially Mission Capable
PSOC	Preliminary System Operational Concept
RCS	Radar Cross Section
RV	Re-entry Vehicle
SAC	Strategic Air Command
SAM	Surface to Air Missile
SLBM	Submarine Launched Ballistic Missile
SLINK	Strategic C^3 Theatre Link (hypothetical example system)
S/N	Signal to Noise
SOC	System Operational Concept
SON	Statement of Need
SPO	System Program Office
SRR	System Requirements Review
SRBM	Short Range Ballistic Missile
SSP_k	Single Shot Probability of Kill
STAR	System Threat Assessment Report
TAC	Tactical Air Command
TED	Threat Environment Description
TFR	Terrain Following Radar
UHF	Ultra High Frequency
VHF	Very High Frequency

1.0 INTRODUCTION

The operational effectiveness analyst is tasked with developing a simulation model for a manned bomber. Which of the dozens of potential adversary air defense weapons should he/she include in the model? Another analyst is examining a satellite communications system for the late 1990's. What proportion of the effort should be devoted to postulated EHF jamming satellites vs. the in-place ground EHF jammers? A third analyst is working on the Advanced Strategic Missile (ASM). The ASM analyst cannot decide whether to include sabotage of the missile base as a realistic operational threat to this system.

These typical problems face operational effectiveness analysts in each strategic system. All can be addressed with a carefully constructed operational threat scenario. This pamphlet describes a procedure for developing an operational scenario encompassing the system's features and mission(s), potential threats, and the various possible system/threat interactions. Such an operational scenario (as depicted in Figure 1-1) will guide the test support group in deciding which threat systems to include, how much effort to devote to each, and how to best integrate the survivability test effort with the rest of the OT&E and DT&E test efforts. The approach in this document is to lay out a sequence of steps the analyst can take to develop the operational threat scenario.

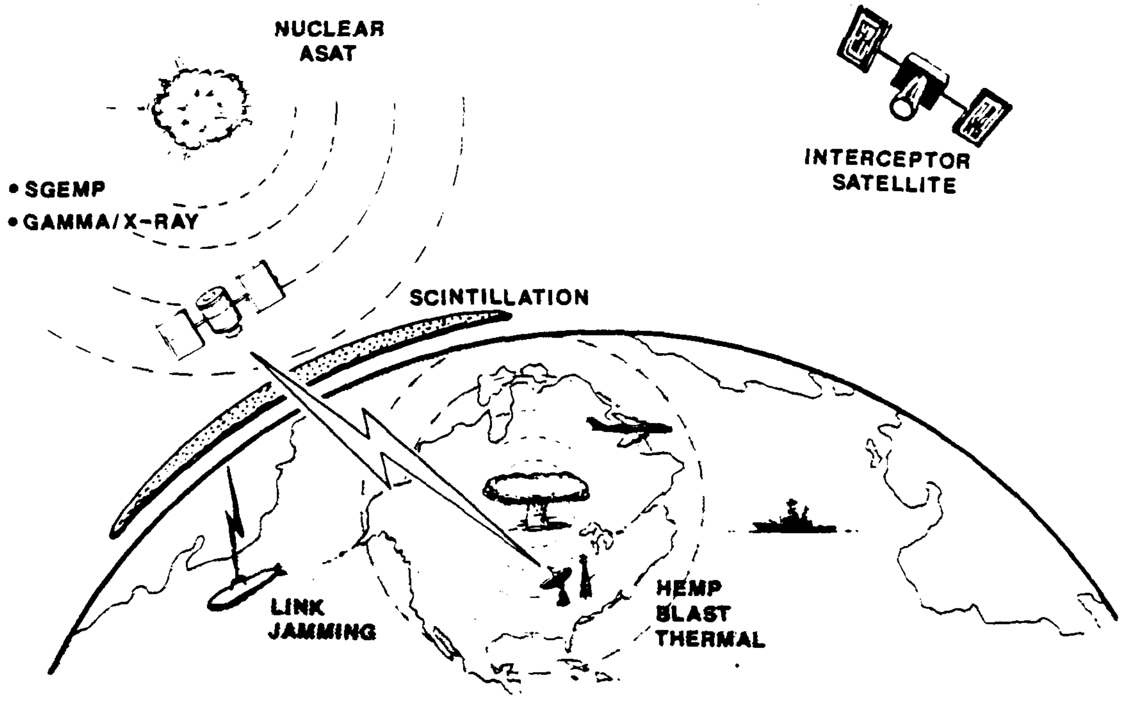


Figure 1-1. SATCOM Operational Scenario

1.1 PURPOSE OF OPERATIONAL SCENARIOS

The IOT&E of any strategic system cannot afford the cost or schedule implications of extensively testing every affectable system attribute. Operational survivability evaluations must, through some logical process, investigate those threat-induced impacts that may significantly reduce performance and the mission success rate. The steps defined in this pamphlet are intended to produce a set of operational scenarios that identify those operationally significant impacts on the system in support of the test approach or test plan.

The key elements of a test approach are identifying what must be tested, how it is to be tested, and what the results will look like. These elements include:

- test issues and objectives
- test asset requirements
- test limitations
- developing methods for test and analysis
- deciding on performance measures
- data required for those measures
- evaluation criteria
- formulating results.

Particular attention should be paid to long lead time items. These may arise from tests requiring unique test support equipment or new models that must be developed in parallel to the system acquisition process. Since this pamphlet and the operational scenarios address survivability issues, those tests and analyses which support survivability objectives are of the greatest concern. These may include joint DT/OT tests, models requiring performance data derived from survivability tests, or analyses developed to handle specific operational survivability problems.

In the simplest terms, an operational scenario is an outline of the conflict from the point of view of the system under test. It describes the mission of the system, where it will be, and what it will be doing, and when. The scenario also contains the adversary war plan for attacking the system. This attack plan includes the threats, how they are employed, the characteristics of the threat (range, accuracy, etc.), where and how the threat will attack the system. These two elements -- the system mission and the threat -- are the foundations of the operational scenario. From that starting point, the analyst can refine the scenario to whatever degree is desired -- ranking especially hazardous mission segments and/or threats, deemphasizing certain threats on tactical or technical grounds, and even including factors such as logistics or weather, if appropriate. So, the operational scenario should show the threats as seen by the system during its mission.

The purpose of the operational scenario is to begin answering the question of what is to be tested. The scenario details the mission and the threats likely to affect the mission, and may even place these threats in priority order. Thus, the scenario is the basis for deciding the importance of evaluating a particular threat/mission interaction. Once the elements to be tested are named, the analyst can turn his attention to how best to test them, and what the results will look like.

The primary reason for developing an operational scenario is to define the parameters of the survivability evaluation of the system. Therefore, to the degree that survivability of the system is critical, the operational scenario should receive increased emphasis. Since most strategic systems are of critical national importance, they are likely targets during an attack, and thus their survivability is important. For a mobile system, designed to escape enemy attack, survivability may be the paramount issue. Operational scenarios can lay the groundwork for various aspects of the OT&E test, including:

- Model or simulation baseline and excursion cases
- Mission outline for performance testing
- Foundation for exercises, field tests
- Resource priority for each threat/mission segment

With this brief introduction to what a scenario is and how it is used, the analyst needs some guiding principles to begin developing the operational scenario.

1.2 GENERAL DIRECTIONS FOR SCENARIO DEVELOPMENT

In developing the operational scenarios, the analyst should keep several factors in mind. These factors relate to the desire for the scenarios to be realistic while focusing on top level, significant systems problems. The details of the process are covered in the remaining sections of the document but a review of the major philosophical points is useful:

- Stay at a top level of the system, its mission and the threats to prevent bogging down in potentially changeable details.

- Depending on the system, the scenario may include 1 vs 1, few on few, nation on nation, or a combination of all levels of detail. The level of aggregation should be the highest that includes the important system threats.

- More than one scenario may be required for the system. In the case of a strategic bomber with multiple missions, different scanarios should be constructed to effectively cover the range of system/threat combinations.

- Operational scenarios are not simply restatements of the threats but tie the possible threat applications to system missions and functional impacts.

- The scenarios are not static and should be reexamined periodically to identify major system operational or design changes, and evolving threats against the system.

- The scenarios are most easily demonstrated through simple examples such as timelines with system missions or functions correlated to threats. A notional example is provided at the end of this section.

- The final results of the evaluation are typically driven by the scenarios so the analyst should realize their importance as the process is begun.

- The operational scenario can be developed at any point in the OT&E planning process. This pamphlet recommends that an intial operational scenario be developed to support the test approach of the system, and that this scenario should be refined during each of the later phases of the OT&E planning and execution.

- The level of detail of the scenario should correspond to the needs of the system, as well as to the phase of the OT&E process. Major, multimission systems will have more complex threats and timelines than simpler systems.

- Be conservative in the incorporation of issues, i.e., do not be too quick to discard a potential operational threat. However, strive to use validated threats.

The importance of the scenarios leads to one significant caveat in this procedure as well. The analyst's responsibility to develop realistic operational scenarios should be tempered by his understanding of the threats and systems. The analyst must refrain from the temptation to generate intelligence information during the process. Whenever and whereever confusion or conflicts develop during the scenario procedure, the analyst should use the resources available to AFOTEC such as DIA, FTD, AF-IN, XPQ, tech advisors, using commands studies and intelligence groups, or contractor support to assure the greatest fidelity of the scenario information. The operationally realistic scenario relies on the best application of valid, verifiable threats, their effects and their appropriateness of use against systems. The generation of "what-if" scenarios defocuses attention and potentially wastes valuable resources.

1.3 OVERVIEW OF SCENARIO DEVELOPMENT PROCESS

An example may help illustrate the process detailed in this pamphlet. We will use the example introduced in this section as a continuing thread through the remainder of the pamphlet. This section describes the output of each of the three steps in the development process; the chapters that follow show how the output is developed.

The development process is described in the flow diagram of Figure 1-2. We will use this diagram to guide the reader throughout the remainder of the pamphlet. The next several paragraphs describe the steps in the flow diagram. This description is followed by an application of the process to our notional mobile C^3 system.

The first step in the scenario development process is to describe the mission of the system. The mission description consists of the objectives and timeline of the mission as well as the description of the system used to accomplish that mission. The mission description may be summarized with a timeline, reflecting the analyst's understanding of the relative timing of system functions that significantly affect the equipment being used or state of the system. This development of the mission description, tying system and mission functions to the mission timeline, is described in Section 2 of this pamphlet.

The second major step in the process is to describe the threat to the system. This step aims at listing the relevant attributes, the number and employment characteristics of all potential threats to the system. The threat description should integrate adversary sensors and weapons systems, leaving the considerations of priority and likelihood for the third step in the process. Section 3 of the pamphlet contains guidance for developing a threat description.

The third and final step is to explicitly apply the threats to the mission timeline to form the operational scenario. The threats can be placed on the mission timeline in a sliding manner. The placement of the threats in relative time should be performed with a couple of limitations. The initiation of attack is governed by

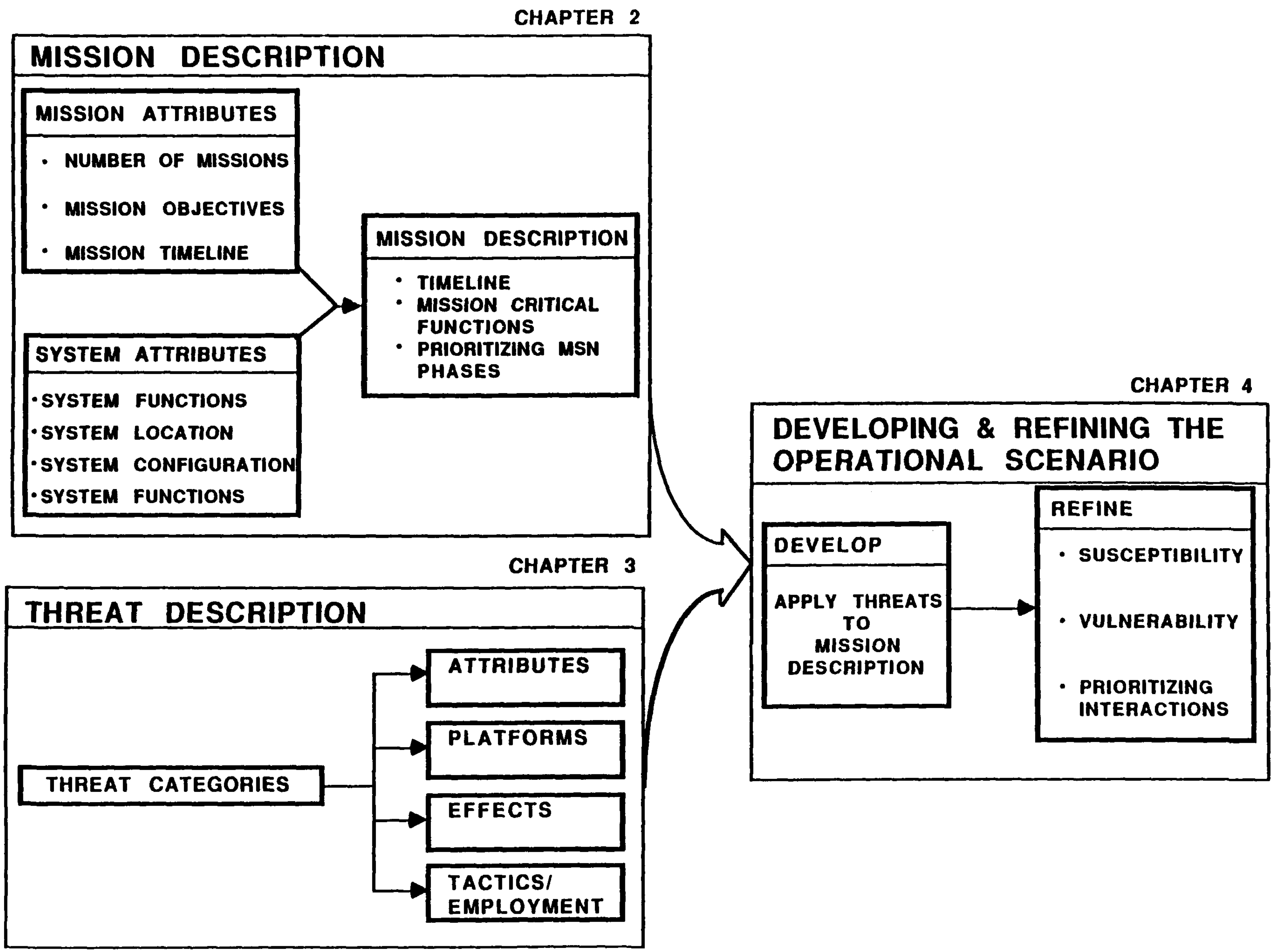


Figure 1-2. Scenario Development Flow Diagram

any threat attribute like flight time or detection time. Since no system is typically physically located adjacent to the threat, this is a reasonable consideration. The threat interaction is thus "kicked off" as the threat reaches the system. The process for applying the threat to the operational timeline forms the first part of Chapter 4.

The initial scenario is then refined by considering the adversary employment concepts and the system factors that make the system a target for the adversary. Perhaps the system is protected against a particular threat effect like radiation, or perhaps the system can and will take action in response to the threat and thus change the relationship between the functions and the threats.

1.4 MOBILE C^3 SYSTEM EXAMPLE OF OPERATIONAL SCENARIO

The hypothetical system used as an example throughout this pamphlet is a strategic mobile C^3 system (SLINK) based in any possible theatre of war, e.g. Western Europe, the Middle East, or Korea. The SLINK system provides survivable linkages from the national command authorities to theatre commanders. The system consists of three trucks containing the communications consoles, power and logistics, and crew berthing. On warning, SLINK deploys from a peacetime staging area to one of several clandestine operating locations. Once there, the SLINK antennas are deployed, communications are established with command centers, and the SLINK system relays messages as required, assuming primary relay duties as other C^3 systems are destroyed. Periodically, the SLINK system redeploys to other locations to preserve location uncertainty. There is only one SLINK system deployed in each theatre. The hypothetical SLINK system is depicted in Figure 1-3.

The fictional operational scenario for the SLINK system is summarized in Figure 1-4. This chart introduces the analyst to the final product we will be developing in the remainder of the pamphlet. The operational scenario depicted by the chart has two main elements: the system mission and the threats applied against it. These are both tied into a conflict scenario shown by the timeline and world events on the top of the chart.

The world event timeline envisions a conflict originating in NATO, escalating to the use of chemical and tactical nuclear weapons, and finally to global strategic warfare. The strategic exchanges are followed by a period of sporadic nuclear exchanges and conventional fighting, and then reconstitution.

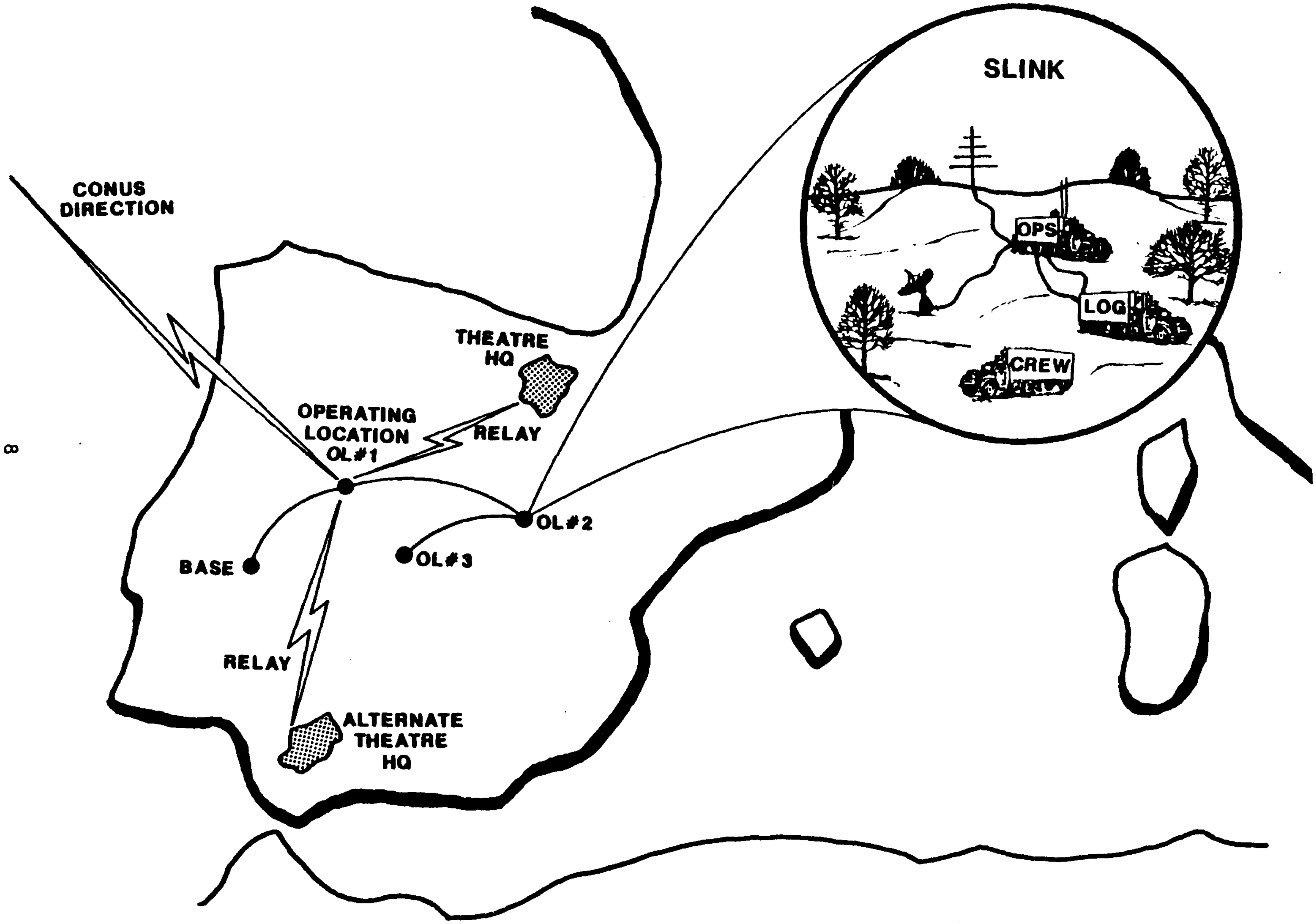


Figure 1-3. SLINK System

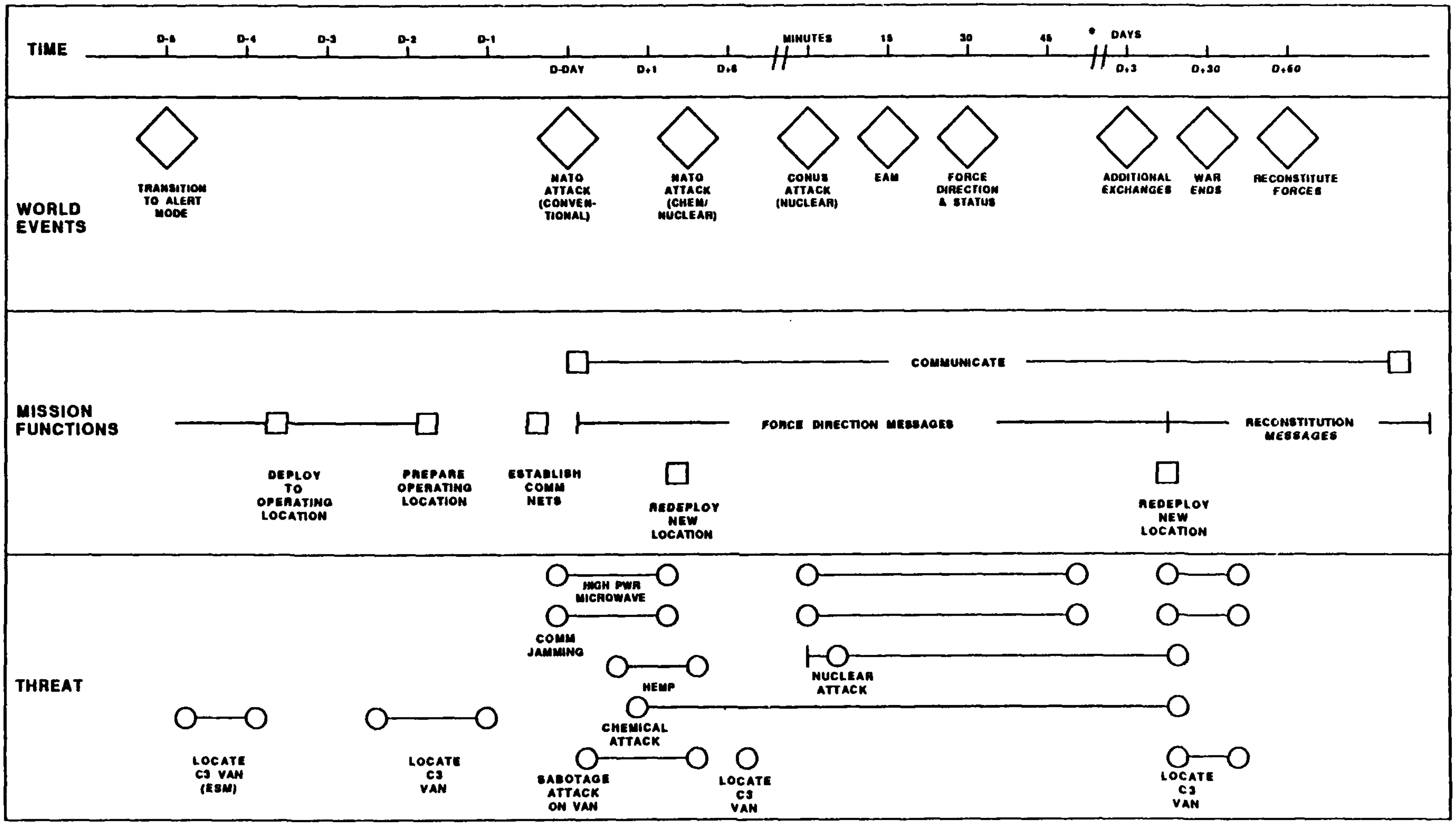


Figure 1-4. Operational Scenario for SLINK C^3 System

The role of the SLINK system is as described previously. On warning, the SLINK convoy deploys to the operational location in each theatre and prepares the location for communicating. As shown in Figure 1-4, just prior to D-Day, the SLINK system has dug in and established its communications links. Once the war starts, the SLINK is needed for communications -- first with force direction and management messages during the conflict, and then for reconstitution messages.

From the point of view of the SLINK system, the major threats during the conflict span the spectrum from sabotage (unconventional warfare) attacks to tactical nuclear weapons. As tensions increase, the adversary can be expected to expend more resources locating priority targets and gathering communications intelligence. Just prior to the adversary's attack on NATO, they attempt to negate our C^3 facilities by a combination of physical attack, and by communications jamming. As the conflict escalates to chemical and nuclear exchanges, so do the attacks on the SLINK system. During the course of the conflict, the adversary is forced to re-locate the SLINK system each time it redeploys to a new operating location. Obviously, the communications jamming threats and attacks can only be prosecuted when the adversary locates the SLINK system (electronically or physically). The next chapter describes the first step in developing an operational scenario -- writing the system mission description.

1.5 ORGANIZATION OF THE DOCUMENT

This introductory section has introduced some general concepts common to all steps in the scenario development process, and introduced the process itself with a hypothetical mobile C^3 system (SLINK). Sections 2.0 through 4.0 discuss the three major steps in the scenario development process -- the system mission description, the threat description, and the mixing and prioritizing of the mission and threat to form the operational scenario. Each of these three major steps is supported by a hypothetical mobile C^3 example with isolated additional examples from other strategic system types, where appropriate. The final section, 5.0, briefly discusses the importance of integrating operational survivability requirements (tests, analyses, and models) with the total system OT&E and summarizes the process. We have included two appendices: a listing of Air Force systems with nuclear survivability criteria, and a sample outline of an operational scenario.

Obviously, no pamphlet can hope to address all the issues peculiar to each strategic system type. Instead, this effort is aimed toward the types of questions that must be answered by each analyst developing operational scenarios. Also, operational scenarios are almost always classified, containing as they do system capabilities, operational plans, and threat descriptions. To keep this pamphlet unclassifed, notional examples are given rather than actual systems and threats. The reader should examine the scenario documents in the references for concrete examples of actual operational scenarios.

2.0 SYSTEM MISSION DESCRIPTION

2.1 INTRODUCTION

The description of the system mission is the first step in the operational scenario development. The mission description contains the objectives and timeline of the mission, details of the functions the system must perform to accomplish its mission, the timing of those functions, and the location and configuration of the system at the time the functions are performed. The mission description is written first because it represents the "target" for the adversary threat. It forms the basis to which the threat is applied, and the criticality and placement of the mission elements determine the relative success or failure of the adversary's subsequent attempts to degrade or abort it. Figure 2-1 shows the mission description step in the scenario development.

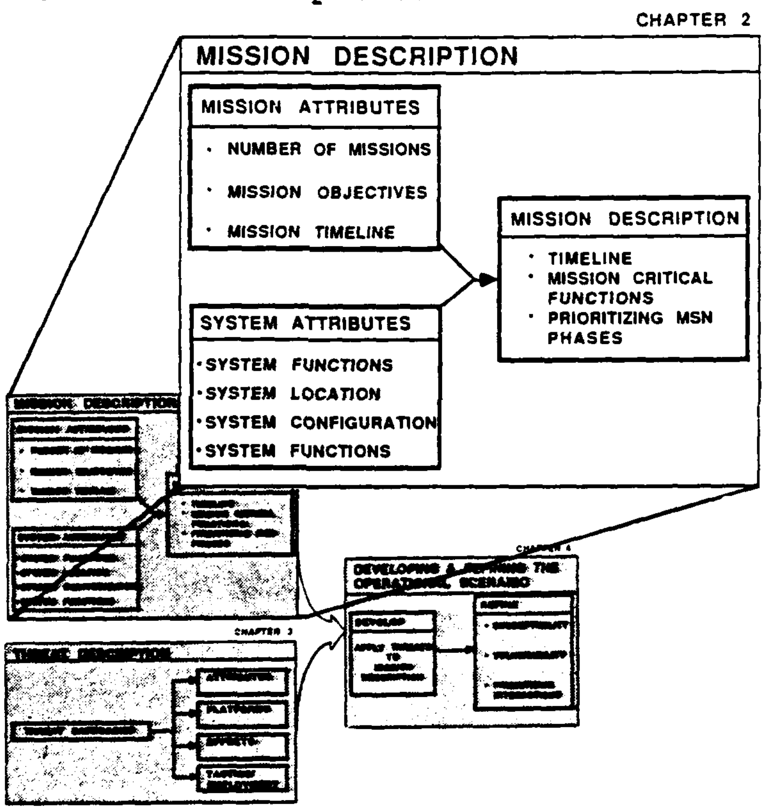


Figure 2-1 Operational Scenario Development Process (Mission Description)

As in all steps in this process, the description should be started as early as possible in the OT&E of the system, and may be done in gross or fine detail. The remainder of this section describes the sources of data available to the analyst in writing the mission description, some guiding principles to observe, and the general form of the mission description. The section finishes with a sample mission description for our SL K C^3 system example.

2.2 DATA SOURCES

Data for compiling the mission description should ideally come from the user of the system. The user initiates the need for the system, but does not always provide the detail desired by OT&E in the description of the operational mission. Therefore, the analyst should be prepared to postulate some details of the mission description from all available data and confirm these with the user. Among the sources of user mission data are:

- Preliminary / System Operational Concept (PSOC/SOC)
- Justification for Major System New Start (JMSNS)
- Statement of Need (SON)
- User Mission Planning Data (operational unit)
- User or AFCSA Force Effectiveness Studies
- Mission Documents for Similar Systems
- Nuclear Criteria Group Secretariat Mission Studies

In addition to the description of the mission, the analyst must also describe the system accomplishing the mission. The best source of system description information is the system developer. Sometimes, more than one program office is involved in developing the system. This case is common in space systems, where one office might develop the ground terminals, while another develops the space vehicle and payload. Among the possible documents available from the SPO are:

- System Vulnerability Analysis
- Decision Coordinating Paper (DCP)
- System Requirements Review (SRR)
- System hardware and software specifications
- Mission Critical Equipment Lists
- Design Parameters Reports
- Nuclear Criteria Group Secretariat (NCGS) Criteria Studies
- Mission Critical Functional Analyses
- Failure Modes, Effects and Criticality Analyses (FMECAs)

2.3 MISSION ATTRIBUTES

When defining the mission, the analyst should keep in mind how the mission description will be used. Since the threat is to be applied to this description, the analyst should describe the mission in sufficient detail to allow threats to be accurately placed. To do this, the analyst should define the following attributes.

Number of Missions Many strategic systems have more than one mission assigned. This is especially true of air-breathing systems like bombers and cruise missiles. Typically, these systems have both a strategic and conventional warfare role. Each of the system missions must be identified, and where appropriate, prioritized.

Mission Objectives For each of the missions of the system, the objectives of the mission must be defined. For an ICBM, the mission may be to deliver the XX RVs to the correct target, on time, and within the operational CEP. For a C^3 system, the mission may be to establish and maintain critical communication links throughout the conflict. Or, the system may have several roles. A strategic bomber can be used in SIOP penetration, sea lane surveillance and interdiction, conventional weapon delivery, or cruise missile delivery. Each mission has different objectives. Certainly, the threats will differ.

Mission Timeline This attribute describes the time dependence of the mission functions. It is the sequential ordering of functions in series or parallel segments, separated by time intervals that can range from seconds to months. Examples include the phases of a bomber mission -- takeoff, weapon delivery, recovery, or functions of a C^3 system -- establish comm link, transmit, receive, log off.

2.4 SYSTEM ATTRIBUTES

Once the mission to be performed is adequately defined, the analyst turns his attention to the system designed to perform the mission. While the system and the mission are interrelated, they are not synonymous. On one hand, missions remain the same, while the systems that perform them become more capable, or do it in slightly different ways. For example, the basic strategic nuclear bombardment mission may not have changed much over the last two decades, but the B-1B is both more capable than the B-52, and also performs the mission differently. On the other hand, sometimes older systems are pressed into new mission roles. Again, the B-52 was designed to perform the high altitude strategic bombing mission, but has been used for the low level penetration mission, and has also added cruise missile carrier and sea surveillance to its repetoire.

System Functions Each system performs a variety of functions to accomplish its mission. These functions include communication, navigation, propulsion, threat detection and evasion, target location and weapon delivery. Some of these functions are more important than others to mission success. And, some of these functions may not even be required for some missions. For example, consider the B-1B in the stand-off cruise missile role. Here, terrain following radar (TFR) is unimportant to mission success. In the penetration role, TFR is almost essential to attempt the penetration, especially in weather or at night. Often, complete lists of system functions are prepared by the system contractor in a Mission Critical Function Analysis or Failure Modes and Effects Criticality Analysis.

System Location Geographical location during various phases of the mission location may include altitude and velocity. Location may be precise, as in a fixed C^3 site, or general, as in the orbit of an Airborne Command Post. Too generic a location leads to difficulty in pairing the system with threats; too specific a location may make the pairing nonrepresentative of the general case. System location for the beginning of the mission has quite an impact on the operational scenario as well. The theatre of operations largely determines the types of adversary weapons with the opportunity to attack the system. For systems with a worldwide mission (like our SLINK example) an operational scenario will have to be developed for each theatre.

System Equipment Although the analyst should keep the operational scenario (and OT&E in general) at the top, or system level, he/she will generally need a physical description of the system equipment. Such a description can often be derived from design documents. The system description should include the major functional subsystems, e.g. radar, INS, sensors, communications or EW suite, etc.

System Configuration The physical and functional configuration of the system may be important to how the system interacts with a threat environment. The configuration can include the crew manning state (if any), the attachment of auxiliary devices like generators, the state of the functional elements for a portable system, or the state of power (on/off).

2.5 MISSION DESCRIPTION PROCEDURE

With the mission attributes and a description of the system in hand, the analyst now brings these together to define how the system will accomplish the mission. To do this, he/she should:

- allocate system functions to mission time periods
- consider the importance of each mission function

- consider the importance of each mission time period

As mentioned before, the critical mission functions are the criteria that determine the success of the adversary's attempts to negate the system. The mission phases represent the adversary's window of opportunity to affect those functions. Great detail is not necessary, as will be shown in the examples in Section 2.6, but coverage of the critical functions is required. This section provides general guidelines for structuring the mission description into a form that can be paired with threats later in the process.

2.5.1 Time Dependence -- Operational Timeline

Once the basic functions of the system are defined, it is useful to allocate the functions as critical or noncritical during various stages of the mission's timeline. For weapon delivery platforms, this allocation is usually intuitive and straightforward; for C^3 systems whose functions are continuous, the time/phase allocation may not be possible. In this case, critical decision points or transitional events should be noted.

The system operational timeline is that period of time for which the system's functions are needed. The timeline need not be continuous. For example, a bomber's functions are not needed during the period between recovery and reconstitution, and the second attack order. During the discontinuities in the timeline, system functions may be allowed to degrade or fail as long as repair can be accomplished, or the function can be regained when needed.

Another example of this discontinuity might be a C^3 system that is vital during reconstitution, but is not needed during the attack and immediate aftermath. Applying the mission critical functions to the timeline assists the analyst in determining the allowable outages and recovery times for the system functions.

Figure 2-2 is a typical mission profile for a strategic bomber. The mission phases are defined in terms major functions (takeoff, etc.), location, duration, and altitude. The configuration of the bomber (flaps, bay doors, crew, equipment power status, etc.) can be defined separately for each phase. Note that in terms of time, the bomber spends most of its mission in the cruise configuration. The early portions of the mission prior to cruise occupy a fairly short length of time, and therefore any threat affecting those functions would have a short window in which to attack the bomber.

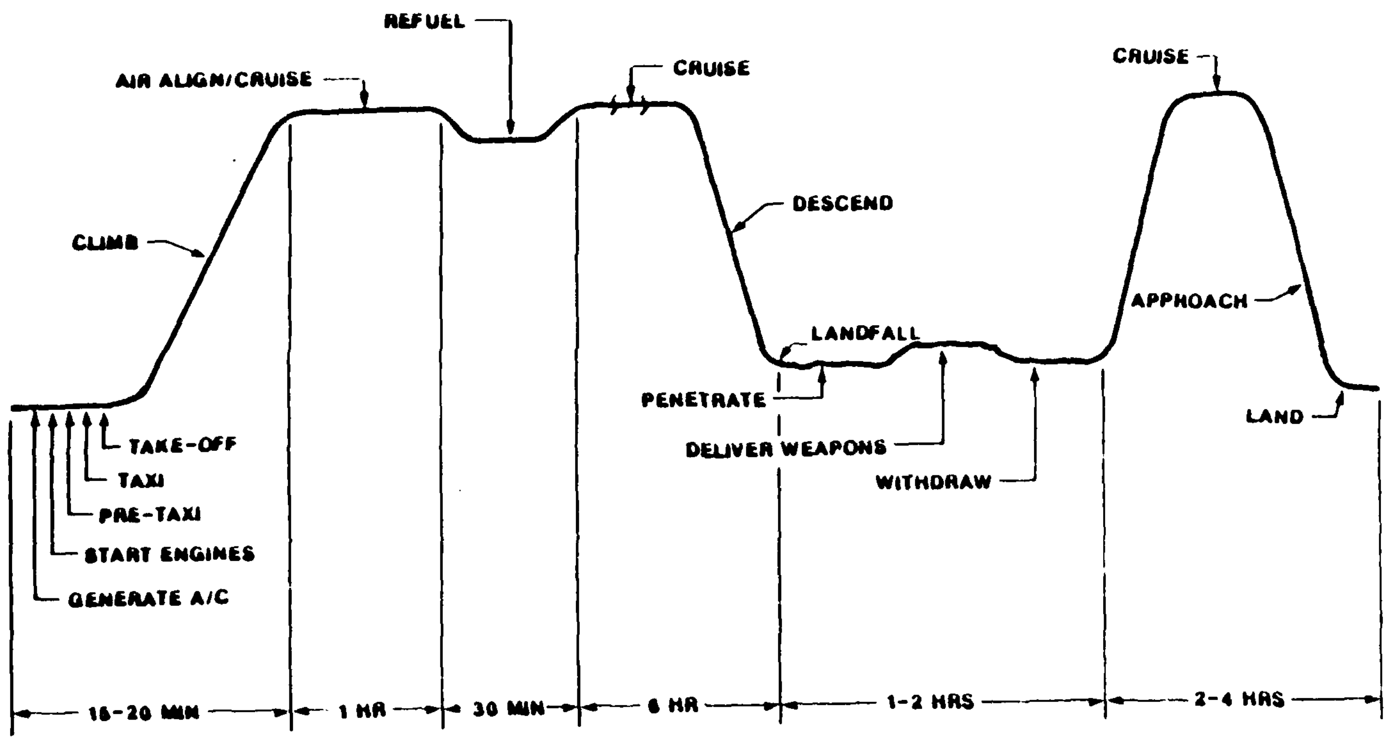


Figure 2-2: Typical Bomber Mission Profile

Figure 2-3 is a typical mission critical function vs. mission phase description for a bomber. The 'Y's in the chart indicate if the function is performed during that mission phase. The last column shows that the bomber function of surviving EMP power off only has to be accomplished during the preflight period of the mission. Similarly, the landing functions and associated equipment are only required at the end of the mission (presumably after the weapons are delivered). If a threat affected the landing system, the mission may have been successfully completed, despite the loss of that function. The importance of the landing function would be decided during the prioritization process and relies on the mission definition, i.e., single or multiple sortie.

2.5.2 Preliminary Mission Critical Functional Analysis

As mentioned previously under the system functions, not all the functions are equal in importance. This step considers whether a function is critical to mission success. For example, a LORAN navigation system in a bomber may not be critical because adequate backup systems exist to perform the same function. Another example is Built in Test (BIT) equipment used during a mission. While sometimes very important, BIT information is often not considered critical to mission success. By using reasoning like this, the analyst can step through the mission functions and decide which are critical to mission success and which are not. Later in the acquisition process, the user logistics groups often develop a study called the Mission Essential System List (MESL). The user uses the MESL to assign a Mission Capable rating to each of his systems. If a mission requires two radios, and the aircraft has only one operational, the aircraft would be rated partially mission capable (PMC) or Not Mission Capable (NMC). The MESL can guide the analyst to what functions are considered important to the user for each mission and which are not.

2.5.3 Prioritizing Missions and Mission Phases

Depending on the system, the missions and phases may be prioritized according to the importance each has to overall user objectives. Prioritizing the missions and functions makes the decision of whether to expend resources on a particular threat/system interaction easier in later stages. For a strategic bomber, the missions might be ranked according to criticality to deterrence. In this scheme, SIOP missions might come first, and the sea lane interdiction mission last.

When all phases of the mission are equally important, or when the functions are not easy to assign to discrete mission phases, it may not be meaningful to prioritize the phases or functions. Suppose that the functions of a radio are to be

MISSION PHASE	MISSION PHASE NUMBER	START SYSTEMS	TAXI	MAINTAIN CONTROL OF FLIGHT	NAVIGATE	COMMUNICATE AND IDENTIFY	RENDEVOUS	REFUEL	EMPLOY EW	LOCATE TARGETS	MANAGE AND DELIVER WEAPONS	MONITOR AND CONTROL OPERATIONS	CONTROL ENVIRONMENT	MAINTAIN CONFIGURATION	LAND/RECOVER	SURVIVE EMP/POWER OFF
STAND ALERT	1.000					Y						Y	Y			Y
UNMANNED	1.110															Y
UNMANNED W/POWER CART	1.120															Y
MANNED W/APU	1.210					Y						Y	Y			
MANNED W/POWER CART	1.220					Y						Y	Y			
MANNED/ENGINE RUNNING	1.230					Y						Y	Y			
START SYSTEMS	2.000	Y				Y						Y				
START W/BATTERY	2.100	Y				Y						Y				
START W/APU	2.200	Y				Y						Y				
START W/POWER CART	2.300	Y				Y						Y				
TAXI	3.000		Y			Y						Y	Y	Y		
TAKE OFF AND CLIMB	4.000		Y	Y	Y	Y						Y	Y	Y		
TAKE OFF	4.100		Y	Y		Y						Y	Y	Y		
CLIMB	4.200			Y	Y	Y						Y	Y	Y		
ACCELERATE	4.300			Y	Y	Y						Y	Y	Y		
CRUISE	5.000			Y	Y	Y						Y	Y	Y		
CRUISE 1	5.100			Y	Y	Y						Y	Y	Y		
CRUISE 2	5.200			Y	Y	Y			Y			Y	Y	Y		
DESCEND	5.300			Y	Y	Y			Y			Y	Y	Y		
RENDEVOUS/REFUEL	6.000			Y	Y	Y	Y	Y				Y	Y	Y		
RENDEVOUS	6.100			Y	Y	Y	Y					Y	Y	Y		
REFUEL	6.200			Y	Y	Y		Y				Y	Y	Y		
PENETRATE	7.000			Y	Y	Y			Y	Y	Y	Y	Y	Y		
DELIVERY	8.000			Y	Y	Y			Y	Y	Y	Y	Y	Y		
RECOVER	9.000			Y	Y	Y						Y	Y	Y	Y	

Figure 2-3: Typical Bomber Mission Functions vs Mission Phase Matrix

prioritized. Can it be said that transmission is more important than reception, or that decoding is more important than encoding a message? Suppose we try to prioritize message types. In that case, any threat that disrupts more important messages may also disrupt less important messages. So, prioritizing the missions, mission phases, and system functions makes more sense for some systems than others. The analyst should consider each system individually and decide if this step is necessary.

2.6 SAMPLE MISSION DESCRIPTION

This section begins with the elaboration of the SLINK example introduced in Chapter 1. We will step through the mission description process just concluded and illustrate each of the steps with the system. We will produce the chart shown in Figure 2-4 -- the outline of the mission description for the SLINK system.

2.6.1 Mission Attributes

For the SLINK system, there is a single mission -- to provide survivable communications links with theatre commanders. This major mission may be broken down into submissions differentiated by the level of command or the technology of the link. For our purposes, we will leave it as a single mission. The mission objectives are two: to survive, and to communicate. Each of these objectives is supported by different types of equipment, performing different functions. If the adversary can destroy the SLINK, or remove its ability to communicate, they will have succeeded in the attack.

The mission timeline is cyclical, as illustrated in the figure. Once the war footing is attained, the SLINK goes through cycles of move--communicate--move, as often as necessary to survive. The actual time increments for these cycles will depend on the system equipment design (modularity, ease of assembly, number of remote connections, vehicle speed and off-road ability, etc.) The time between moves is dictated by the threat intelligence cycle time -- the time to identify, target and engage the SLINK.

2.6.2 System Attributes

The system functions are identified as dot-points in Figure 2-4. For each of the mission phases in the mission timeline, the SLINK performs a unique set of functions. In this example, the functions were developed logically by the analyst, and will be updated with a more complete list when the development contractor delivers the Mission Critical Function Analysis. To prevent gross errors in the function listing, these functions were informally reviewed by the SPO.

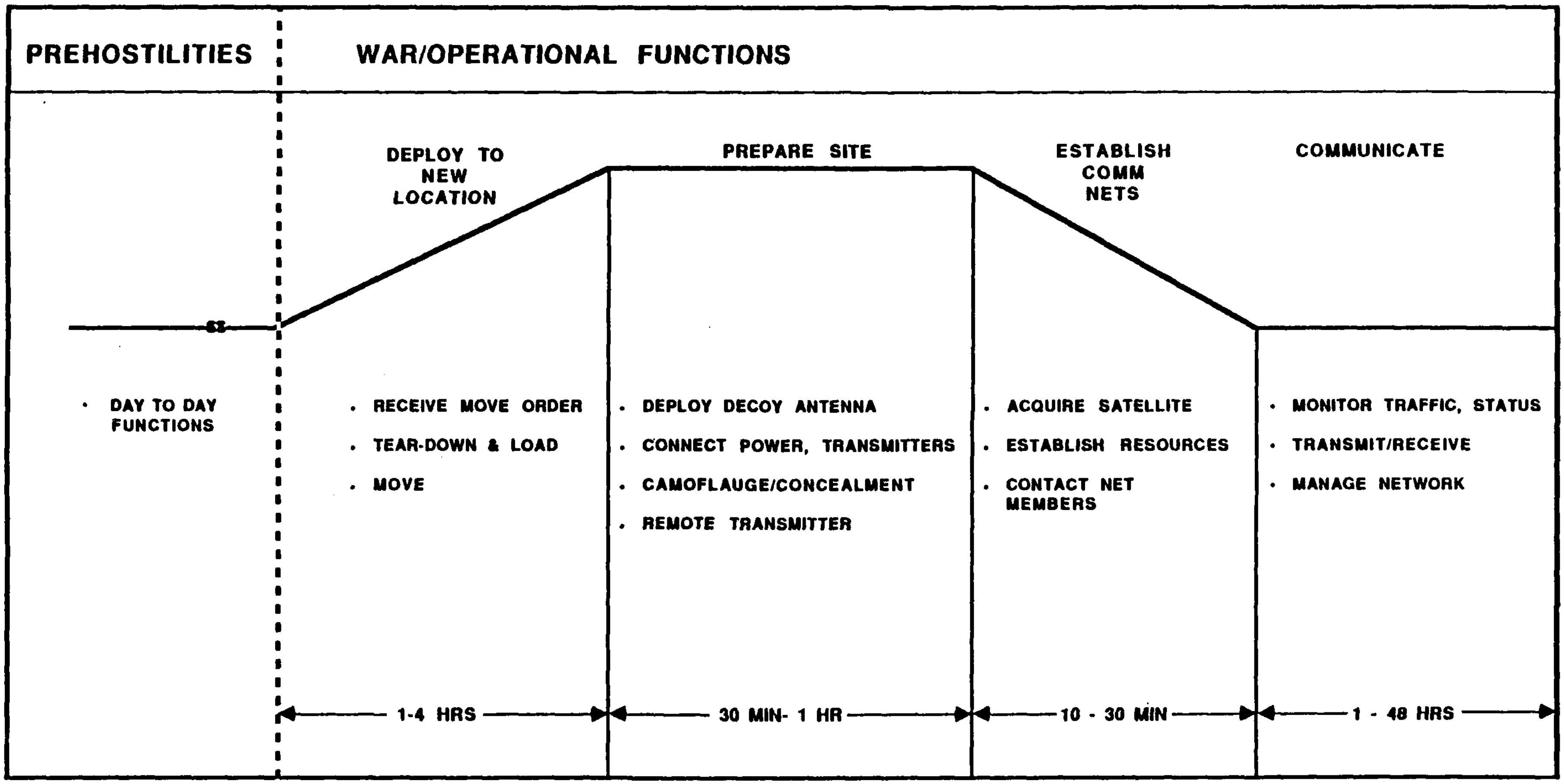


Figure 2-4: C^3 SLINK Mission Timeline

The system locations are preplanned for each theatre. Up to ten locations are chosen and surveyed to advantageously site the SLINK. The locations are listed in a user document attached to the system operational concept. For the purposes of the operational effectiveness analysis, two sites in each theatre are chosen, representing the sites most vulnerable to adversary conventional attack and jamming. Presumably, the SLINK system will operate as well or better in the eight remaining less vulnerable sites.

The system description for the SLINK was derived from a variety of hypothetical documents, including the specifications, several system briefings published by the developer, and a logistics analysis describing the BIT provisions for each major subsystem. For the operational scenario, the key aspects of the system design were the low radar observable vans, the sidelobe suppression on the communications antennas, and the characteristics of the active decoy antennas deployed within a kilometer of the actual antennas.

The configuration of the system is also described in the system description documents. There are two major configurations of interest to the operational scenario development. The first was the standard full configuration, with all vehicles deployed at the operating location, all decoy antennas arranged some distance away, and the entire base covered with camoflauge netting. The second configuration, the stealth configuration, involves only the transmitter truck and antenna located on the operation site. The remainder of the vehicles are to be located some distance away, and any required interface between the transmitter and other vehicles was done by landlines and shuttles. The transmitter truck is masked by available terrain features, is heavily camoflauged, and employs strict emission control to minimize intercepted radiations. These two configurations are important because the target presented to the adversary is markedly different between the two. As will be seen in the next section on the threat, complete descriptions of these configurations will have an important impact on which threats can engage the system.

2.6.3 Mission Description Summary

Now that the mission has been described, and the system discussed, the two elements will be brought together to complete the mission description.

As shown in Figures 2-4, the system functions have already been allocated to the mission timeline. The allocation was done through a logic flow, and is subject to change as more information develops on the system.

Since this is a preliminary mission description, no great effort will be made to prioritize the mission functions or the mission phases. However, the two paragraphs below will describe the line of thought that might be followed in making these priority choices.

At first glance, it might be thought that all the mission functions are mission critical and of equal priority. However, there are at least two listed functions that are not, strictly speaking, mission critical. Both of these functions are in the site preparation phase. If the adversary destroys the decoy antennas, SLINK will still be able to perform its mission functions. While the system is now more vulnerable to the adversary, more attention to emission control, and assuming the stealth configuration may allow SLINK to survive and complete its mission. In the same way, if the transmitter remoting equipment is destroyed or disabled, the transmitter can still be directly attached to the antenna and SLINK will still be able to transmit and receive, although somewhat less survivably. So, these two functions may not be mission critical and will probably be given a lower rating during the prioritization step.

Mission phases in the move-communicate-move cycle also appear to all be of equal priority. While it is true that the SLINK must perform all these phases, the vulnerability to threat classes differ among phases. For example, the SLINK is vulnerable to jammers and electronic detection only when radiating, which it does only in phases 3 and 4. When the SLINK system is moving or preparing a site, it is more vulnerable to conventional attack since it is not camoflauged. We will discuss these issues later, as we fold the threat into the mission description to form the complete operational scenario.

3.0 THREAT DESCRIPTION

3.1 INTRODUCTION

As in the section on the mission description (Section 2) this section on the threat description begins with a list of data sources for the analyst, followed by some general principles to guide the analyst. It then describes the salient aspects of each type of threat considered here: nuclear, conventional, electronic warfare (EW), chemical and directed energy. The section concludes with examples of typical threat trees for the three generic types of strategic systems, and the continuation of the SLINK example. Figure 3-1 shows the outline of the threat description process, and how it relates to the mission description and the final operational scenario.

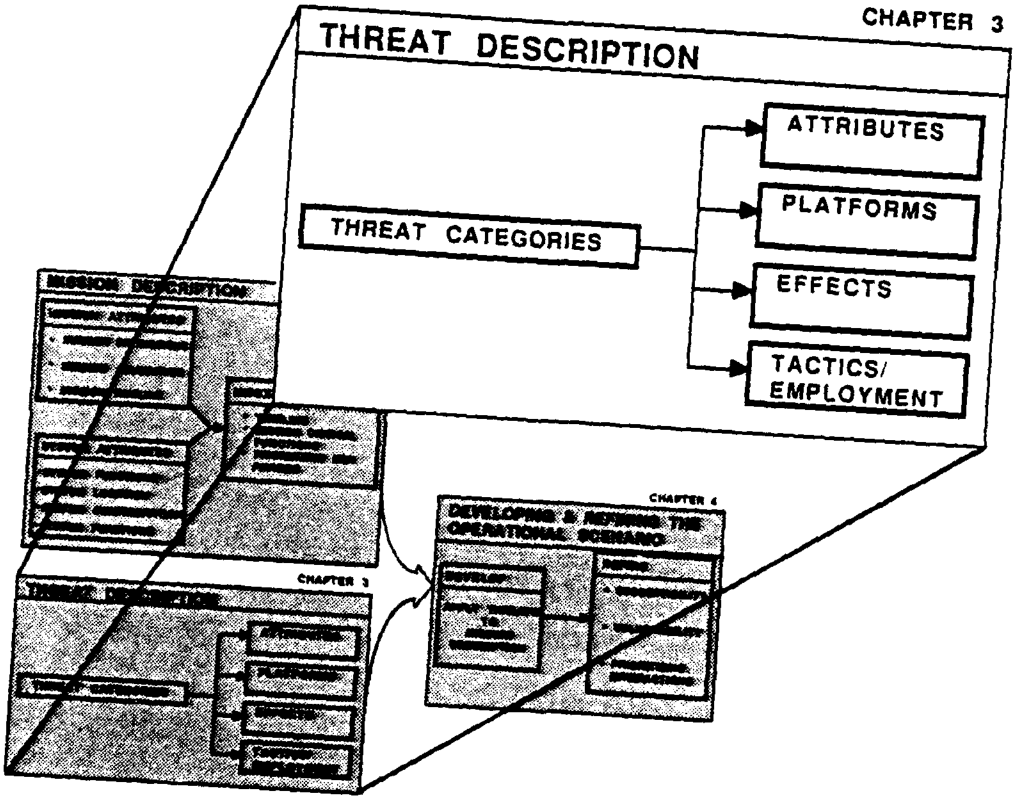


Figure 3-1. Operational Scenario Development Process (Threat Description)

The threat description begins with considering the range of threats that can be applied against the system. Then, for each threat chosen as a candidate, specific characteristics of the threat are defined. These characteristics include various threat attributes like range or power, delivery platforms, threat effects on systems, and employment concepts.

The essence of the threat description is a comprehensive list of reasonable threats against the system. The analyst must research the available information and then place himself in the adversary's shoes to determine how the system and its functions and elements can best be attacked. While doing so, the analyst must simultaneously guard against including unlikely "pet threats" and dismissing validated adversary systems. The refinement of the operational scenario (Section 4) will winnow out some threats that may be tactically or technically infeasible or inefficient for use against the system.

Figure 3-2 is a pictorial of a threat description for an ICBM. It includes all threats that can be employed against the system during each phase of the system's mission. This picture illustrates that although we discuss the threat description as an independent step in the process, the analyst must always keep the mission description just completed in the back of his mind.

3.2 DATA SOURCES

There are many sources of threat data available to the analyst. Often these sources provide conflicting information. However, the analyst must be familiar with the various general and system-specific sources published that concern his system. The analyst's goal in describing the threat is not to create new system threats, but to compile the available information into a concise description of the breadth of threats the system will face. Details will vary from threat to threat, depending on the published sources described below.

3.2.1 Intelligence Community

The analyst's first research into the threat should focus on the information published by the intelligence community. The function of the intelligence community is to describe the threat capabilities of the adversary in sufficient detail so that MAJCOMs and designers can counter the threat. The quality of the threat descriptions will vary from system to system, depending on the types of threats, the time period considered, and the characteristics of the system mission. Sources in the intelligence community include:

- Foreign Technology Division (AFSC/FTD)
- Air Force Intelligence (AF/IN)
- Defense Intelligence Agency (DIA)
- National Security Agency (NSA)
- Army Intelligence
- Army Missile Intelligence Agency (MIA)
- Navy Intelligence (NIS)

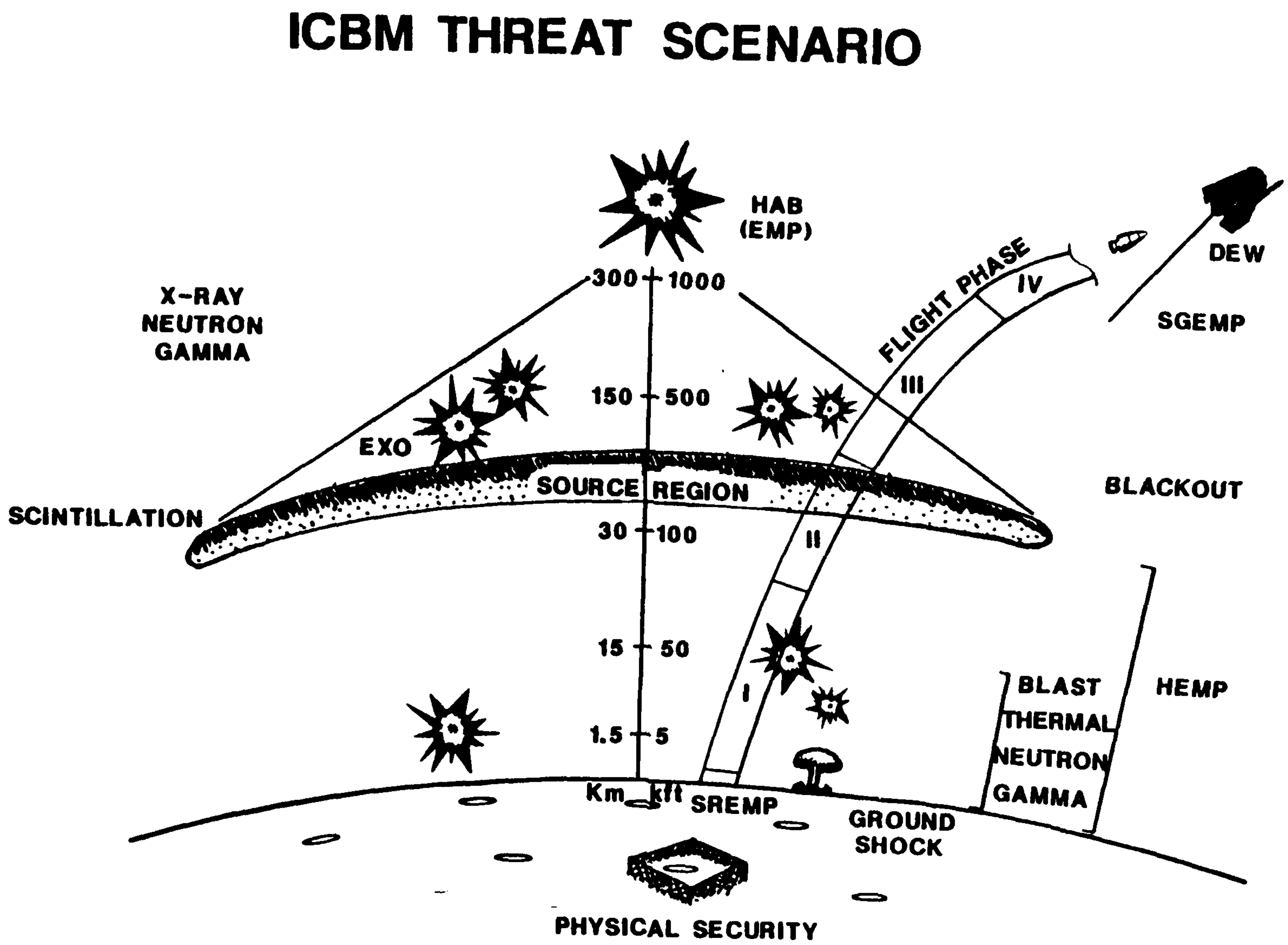


Figure 3-2. ICBM Threat Description

The AFOTEC division responsible for threat information is AFOTEC/XPQ. XPQ maintains a database of threat information published by the above sources, ranging from general to system specific. They also have contacts at the agencies listed above and exist to support the project officer in gathering threat data. XPQ should be the analyst's first stop in preparing the threat description.

Among the most useful documents XPQ keeps are the FTD-published Threat Environment Descriptions (TEDs). TEDs are published for general system types, as well as for specific systems. The General TEDs are designed to support multiple systems or multiple operations concepts. They are used in Mission Area Analyses and concept studies.

The six general TEDs available are:

- Tactical Air
- Space Systems
- Mobility Forces
- Electronic Combat
- Strategic Defensive Systems
- Strategic Offensive Systems

The TEDs have 17 appendices that address specific threat areas. These Appendices are:

APPENDIX I	Non-Military Threat
APPENDIX II	Ballistic Missile Systems
APPENDIX III	Bomber Aircraft
APPENDIX IV	Fighter Aircraft
APPENDIX V	Surface-to-Air Missile Systems
APPENDIX VI	Surveillance Radars
APPENDIX VII	Antiaircraft Artillery Systems
APPENDIX VIII	Electronic Warfare Systems
APPENDIX IX	Command, Control and Communications
APPENDIX X	Soviet Naval Surface Combatants
APPENDIX XI	Military Weather/Climate and Geographic Considerations
APPENDIX XII	Land Attack Cruise Missiles
APPENDIX XIII	Combat Sustainability (Theatre Logistics)
APPENIDX XIV	Space Systems
APPENDIX XV	Soviet Tactical Targets Characteristics
APPENDIX XVI	Chemical-Biological Warfare
APPENDIX XVII	Combat Helicopters

The general TEDs provide an excellent background for the analyst in the threat areas of interest for the system. The specific TED for the system (if published) will draw on the general TED and apply the threats to the particular system. Questions concerning the TEDs can be directed to AFOTEC/XPQ or HQ Foreign Technology Division (FTD/TD) AV 787-3141.

Additional sources of intelligence information include the following classes of documents.

- System XXX System Threat Assessment Report (STAR)
- National Intelligence Estimates
- Defense Intelligence Agency Projections for Planning
- Army Military Intelligence Appraisals
- Intelligence Studies for Similar Systems

3.2.2 User Studies

The MAJCOM system user often has performed force effectiveness studies, sometimes in conjunction with the Air Force Center for Studies and Analysis (AFCSA). These studies require assumptions about threat capabilities and employment, and may be very useful to the analyst since they can represent the user's viewpoint. Often the MAJCOM plans directorate (XP) can guide the analyst to these studies, or the analyst can contact AFCSA directly.

The user SON and SOC often have a digest of the threat contained in them to justify the need or use of the system. Although this information is often not detailed enough for use in this process, it identifies the classes of threats of concern to the user.

3.2.3 Development Community Data Sources

The development community comprises the Air Force Requirements branches, the product divisions of AFSC (the SPOs), technical support contractors, and the development contractors. These organizations have the responsibility of translating the intelligence threat into a set of design specifications for the system that are cost effective and technologically feasible. Ideally this process results in a system that can withstand the threat and meets the user's performance requirements. In reality, survivability tradeoffs are made to achieve cost savings, increased performance, achievable technology, or maintainability. These tradeoffs are often lucrative areas for OT&E investigation, since such tradeoffs may impose an unacceptable penalty to the user in terms of the performance of the system.

The process the SPO uses to translate intelligence data into system design specifications varies from SPO to SPO. However, the process is usually documented and the analyst should press the SPO for its rationale in developing the specifications. The SPO is responsible for developing the System Threat Assessment Report (STAR), and this document is a good place to begin the threat investigation. At the very least, the analyst can discuss the process and reasoning used with the applicable elements of the SPO organization.

In the nuclear threat area, a unique organization exists that can greatly assist the analyst in translating the nuclear threat information into an operational threat description. This organization is the Nuclear Criteria Group Secretariat (NCGS) attached to the Air Force Weapons Laboratory (AFWL) at Kirtland AFB, NM.

The NCGS prepares reports summarizing the nuclear threat to the system, the application of the threat to the mission timeline, and the hardness levels the system should be designed to, to create a nuclear survivable system. These reports document the analysis and are used in specifying the nuclear weapon environment criteria for the Air Force systems. These reports are usually prepared early in the system development cycle (hopefully before its specifications are developed) and are authorized under AFR 80-38 (Air Force Survivability Program).

The NCGS has the responsibility for conducting the analysis and preparing the NCG report. The analysis process followed by the NCGS is similar to that described in this pamphlet with the exception that the process normally stops at the mission profile point. Early in the system development process only generalized mission profiles are normally available so the criteria are developed using these mission profiles and established threats. The analysis process then determines operational threat engagement scenarios for each phase of the mission. A matrix of weapon yields and distances to each appropriate nuclear environment is developed using possible hardness levels of the system. An analysis is then performed to choose optimal hardness levels consistent with cost, hardening technology and other survivability techniques. The NCGS reports for MILSTAR, Peacekeeper and B-1B are good examples of NCGS products.

The NCGS process is operationally oriented in that the analysis considers the threats to the system and the specific missions of the system as defined in the system operational concept. However, since the criteria study may be several years old, and since the charter of the NCGS is different than AFOTEC's, the NCGS report for a system should only be considered as a starting point for the development of the operational threat description. In addition, the criteria developed by the NCGS are not always used by the system program office and may have been modified.

HQ USAF/RDQI (Requirements) maintains a database for all systems with nuclear hardening criteria, analysis, tests, etc. This database describes the details of the nuclear criteria history for the system and serves as an excellent starting point. Copies can be obtained by calling the PE 64711F program element monitor (currently LtCol Bill Beekman). Systems covered in this document are shown in Appendix A. The threats and mission should be reevaluated periodically with current threat and system data. Although AFR 80-38 currently only requires such studies for nuclear weapons effects, it is currently being modified to include a broader set of threats including the evolving directed energy weapons.

3.2.4 General Adversary Strategy and Tactics

While developing the description of the threat, the analyst should become acquainted with the way the adversary thinks about warfare. Although the analyst need not become an expert in adversary force employment, he should familiarize himself with the basic tenets of strategy. Among these are the classic elements described in JCM 1-1 as the elements of warfare. They include:

- Economy of Force
- Mass
- Speed
- Surprise
- Control and Direction

The basic uses of the threat weapons are important to the analyst, since this use dictates if and how the weapon will be used against the system. In the nuclear arena, the analyst should understand the general target set for SLBMs and why they are not effective against hardened targets. The analyst should know the basic timeline for employment of ICBMs and the general characteristics (yield and accuracy) of the various systems. Attributes like these for each of the general classes of threats are listed in following sections of this chapter.

3.3 PRINCIPLES

In developing the threat description, the analyst should keep in mind the following set of guiding principles and warnings. Since the threat data may be sparse, conflicting, or frustratingly general, the analyst must remember the goal of the threat description. This goal is to place himself in the adversary's shoes, with the adversary's weapons and strategic thinking, and to describe the threat weapon systems that <u>may</u> be targeted against the system in question. Again, in this step, the objective is an integrated, broad description of the threat, based on validated intelligence sources.

Examining the feasibility of the threat and the effects on the system will be the last step of the operational scenario development process.

3.3.1 Three Elements of Attack

To threaten a system, an adversary must first detect it, then engage it, and finally be able to damage or negate it. These three elements can be thought of as the basic characteristics of a threat system. Not all threats to the system are of the lethal type. The adversary's capability to detect, jam, exploit, or otherwise nonlethally engage the system must also be part of the threat description. Figure 3-3 is a pictorial view of these three elements.

Detection encompasses a system observable and an adversary sensor. System observables include visual, thermal, electronic, magnetic, and acoustic. Adversary sensors include active and passive sensors. Sensor examples include radar, radio direction finders, IR sensors, lasers, acoustic listening devices, and may be found on ships, submarines, aircraft, satellites, ground vehicles, etc.

Engagement includes the ability to physically attain the geometry required to affect the system. For missiles, directed energy weapons and projectiles, engagement includes tracking, aiming/guiding and firing. For example, directed energy weapons must have an unobstructed firing line between themselves and the target. While the firing line may be thousands of miles long for space weapons, this line-of-sight requirement places severe restraints on the three dimensional geometry of the threat and target. For electronic disruptive or listening devices, engagement means being able to receive the transmission, or to place the required amount and type of energy into the system receiver. An electronic listening device is placed at a disadvantage against a system with low probability of intercept emissions.

Damage or negation means that the engagement must affect the system's functions. This effect may be subtle, as in the case of EMP upset, or catastrophic, as in the case of a nuclear detonation or missile impact.

Keeping these three concepts -- detection, engagement, and damage -- in mind assists the analyst in covering the full range of threats against the system, and not narrowly focussing on one technology or one exploitable aspect of the system.

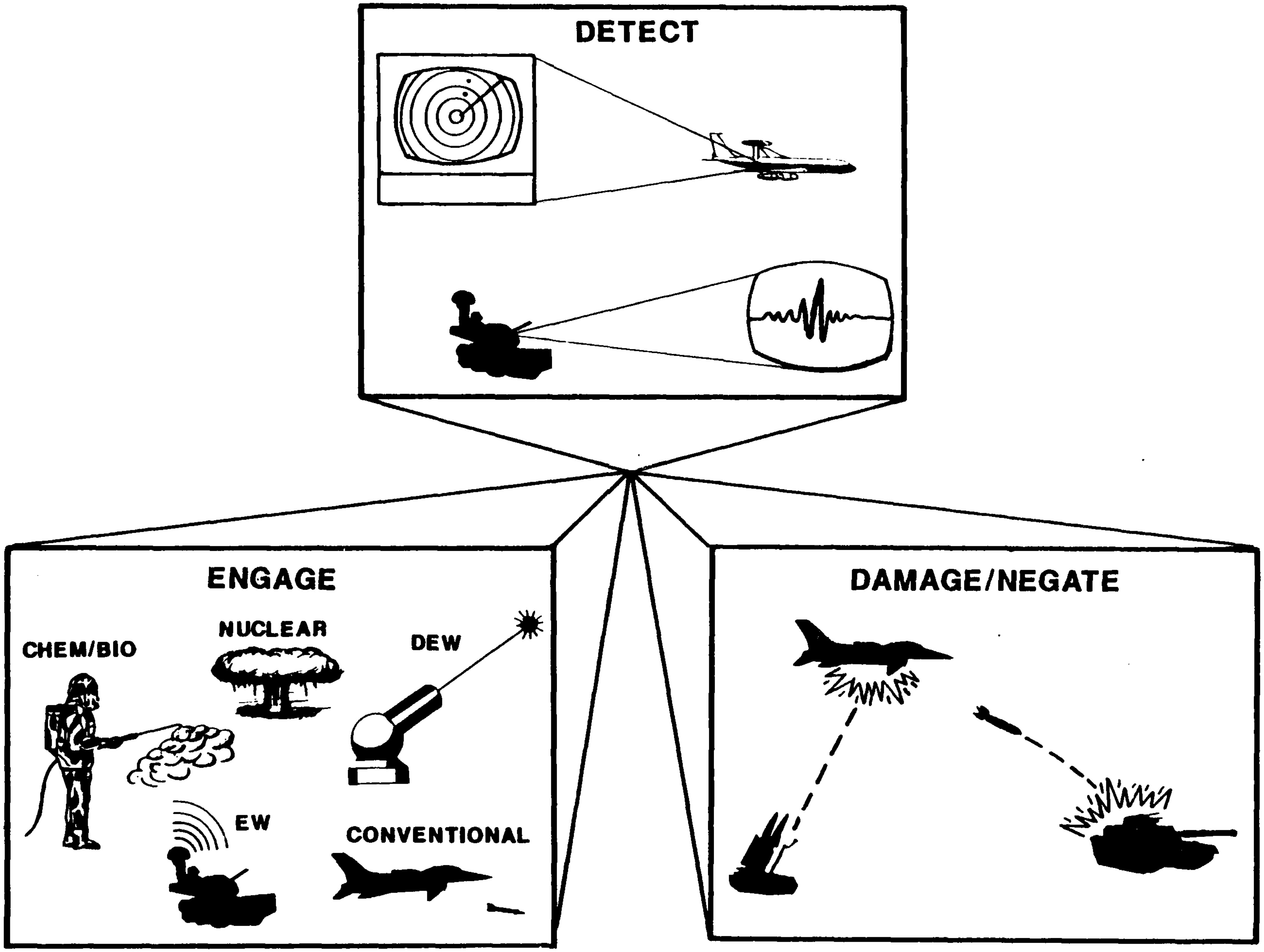


Figure 3-3: Three Elements of Attack

3.3.2 Adversary System Employment Concepts

The adversary will employ the threat weapons according to the target set, weapon capabilities, opportunity, and general strategic principles. The intelligence approach to enemy intent is usually to describe capabilities, and assume that these capabilities will be used whenever feasible. This is unfortunate for the analyst, since there are seldom well accepted descriptions of enemy intent. For example, the adversary may have the capability to target all airfields with runways over 10,000 feet long in a first strike. If they did so, this would affect the ability of strategic C^3, tanker, and bomber aircraft to recover to the CONUS. Whether they would, in fact, do so is the question of intent. The analyst must face difficult questions like these in developing his operational scenario. The analyst must strive to understand intent, since this governs the application of the threat to the system, but not rely on intent to greatly constrain the threat employment.

3.3.3 Threat Types

In general, intelligence postulates three types of threats to the system. The first of these threats are those that are already fielded or near fielding. These inplace threats can usually be used against the system, or a variety of other systems.

Developmental threats, the second type mentioned in intelligence estimates, are those that are expected to be deployed during the useful life of the system. The developmental threats can be very important to the survivability of the system since they usually represent greater capabilities. From the analyst's point of view, these are more difficult to address, since the increased capabilities are often not exactly known, and may change during the OT&E process.

Reactive threats, the third type, are those that are developed specifically to counter vulnerable aspects of the system under development. By their nature, reactive threats are even less well defined than developmental threats. The capabilities of reactive threats depend on the adversary's concept of the system's vulnerabilities, the priority the adversary places on countering the system, and his ability to do so. Examples of reactive threats include new satellite sensors to keep track of mobile systems, faster or different wavelength jammers for new communication systems, earth penetrating nuclear RVs to counter hard silos, or more sensitive radars to overcome low RCS technology. In general, the analyst should devote more effort to the in-place threats and developmental threats while keeping reactive threats under consideration until more intelligence information develops. Reactive threats may become a major danger to the system, but the analyst must obtain reliable information on the threat's advanced capabilities before centering the analysis around them. The adversary is not ten feet tall, and operates under resource and technical constraints as we do.

3.3.4 Integrated Threats

As mentioned above, the adversary must complete three activities to affect the system: detection, engagement, and negation or damage. The interaction of one threat with another can cause the system to be more exposed to the effects of another threat. For example, if the adversary could keep US ICBM's in the silo with a barrage attack of nuclear blast and thermal effects, the ICBMs are at greater risk to incoming direct-attack RVs. If adversary jamming forces greater numbers of transmissions or higher power transmissions, it may make a C^3 system more susceptible to ELINT and subsequent targeting. Therefore, it is important to operational realism to describe the total breadth of threats that can be targeted against the system. The analyst may not understand the interactions at this point in the OT&E, but he/she should make provision for investigating them by including all applicable threats.

3.3.5 Conservatism

The principle of keeping all threats under investigation in the threat description step follows from the principles stated above. It is a fairly easy matter to dismiss threats (as described in the following chapter), but it is more difficult to add threats back into the process when they have been prematurely removed. Threats should be considered valid unless strong evidence indicates otherwise. By adhering to this principle, the analyst forms a defensible, documented trail that leads to the final operational scenario.

3.4 NUCLEAR THREATS

In this section, and the next four that follow (3.5-3.8), the characteristics of various threat types are described. These listings of characteristics are obviously not exhaustive, but provide a checklist of items that the analyst should include in the threat description. Obviously, the level of detail required depends on the stage OT&E has reached. For a test approach, the descriptions may include only general system types and characteristics. For test planning, more detail is needed to identify specific test data requirements. During test execution, even more detail is needed to actually simulate the threats of interest. A well written operational scenario can be a tool to identify areas where more data is needed to conduct the OT&E. The scenario can include lists of data requirements identified during the development process. These shortfalls can be identified to the intelligence and range development communities as validated OT&E requirements.

3.4.1 Attributes

Nuclear weapons can be characterized by several attributes. These include:

- Yield
- Range
- Accuracy (CEP, etc.)
- Number
- Warhead output characteristics (X-Ray yield, etc)
- Burst Height
- Launch timeline with respect to mission

3.4.2 Platforms

Weapons platforms are divided into those capable of strategic (CONUS) delivery, and those capable of theatre (NATO, Korea, PACAF, etc.) delivery.

CONUS	Theatre
ICBM	SRBM/SLBM/IRBM
SLBM	Artillery
Bomber	Cruise missile
Cruise Missile	Bombers
	Tactical Aviation
	Surface-Surface Rocket
	Unconventional Warfare teams
	Air Defense Weapons

3.4.3 Effects

Volumes have been written about the effects of nuclear weapons, and the interactions of the explosion with the environment and the system are exceedingly complex. For the purposes of this pamphlet, the major effects are listed in Figure 3-4, according to the type and deployment area of the US system.

3.4.4 Employment

Nuclear weapons are employed in various manners, the most common of which is direct attack of a target. They can also be used to deny areas (barrage, radiation), generate high altitude EMP, and to disrupt communications (blackout, scintillation). The direct employment of nuclear weapons depends mainly on available resources,

System Location	Environment									
	High Altitude EMP	Source Region EMP	System Generated EMP	Blast	Thermal	X ray	Neutron Gamma	Ground Shock	Total Dose	Scintillation
Subsurface	x	x					x	x	x	x
Surface	x	x		x	x		x	x	x	x
Airborne	x			x	x		x		x	x
Space		x	x			x	x		x	x

Figure 3-4: Summary of Nuclear Weapons Environments

hardness of the target vs accuracy and yield of the weapon, knowledge of the target location, and the priority of the target compared with other possible targets. ICBMs are generally used for hardened and high value targets, while SLBMs are used for soft, area, or time sensitive targets. Bombers service remaining non-time sensitive targets and conduct damage assessments. Space systems may be vulnerable to nuclear ASATs launched on modified ICBMs.

Tactical nuclear weapons follow the same general principles as strategic nuclear weapons: high accuracy weapons are used against hardened targets, and less accurate, shorter time of flight weapons used against soft, area, and time sensitive targets. For example, IRBMs might be used against fixed, hardened command posts, while nuclear mortars or artillery might be used against troop or vehicle concentrations.

3.5 CONVENTIONAL THREATS

Conventional threats include weapon delivery from aircraft, infantry, tanks and artillery, air defenses, unconventional warfare teams, agents, and terrorists. This wide range of threats makes it difficult to say anything general about them. However, they are also not the primary threat to strategic systems.

3.5.1 Attributes

The attributes of conventional forces include;

- Weapon type(s)
- Range
- Accuracy (SSP_k, CEP, etc.)
- Rate of fire
- Altitude limits (low and high)
- Explosive size and warhead type
- Number of personnel and weapons
- Objectives (destruction, harrassment, ransom)
- Transportation
- Communications
- Rate of Advance

3.5.2 Platforms

Conventional threat platforms range from the individual human to bomber aircraft.

3.5.3 Effects

The effects of conventional threats are generally mechanical in nature. The weapons are kinetic energy or high explosive, and depend on deformation, implosion, or penetration for their effectiveness. These effects are generally well understood and can be protected against with suitable defenses (active and passive), intrusion detection and security force responses, etc.

3.5.4 Employment

In general, CONUS-based strategic systems are not targeted by adversary ground forces or conventional aircraft. The major conventional concern of CONUS forces will be sabotage teams and terrorism. Strategic bombers and other strategic aircraft may face air defense weapons as well as the unconventional warfare threat on the base. ICBMs also face the physical security risk from unconventional warfare teams.

In theatre, an element of a strategic weapon system (cruise missile, bomber, or C^3 node) will face the full range of adversary ground force threats arrayed against the US. The TEDs should be consulted for further information on these threats.

3.6 ELECTRONIC WARFARE THREATS

Electronic warfare, or electronic combat threats can be divided into two groups: passive or electronic support measures (ESM -- ELINT, DF, Radar etc), and active electronic countermeasures (ECM -- jamming, spoofing, deception).

ESM is defined as actions taken to intercept, identify, and locate radiated electromagnetic energy. ESM includes direction finding, interception, exploiting, and detecting. Sources differ as to whether sensors such as radar should be included in this category, but they will be for the purposes of this description.

ECM is defined as actions taken to prevent or reduce the adversary's use of the electromagnetic spectrum. It includes jamming, electronic spoofing and deception.

3.6.1 Attributes

<u>Electronic Support Measures</u>

Characteristics of ESM threats are related to their ability to sense, follow, and interpret the emission of the system. In engineering terms, sensing is described as signal to noise ratio (S/N). In operational terms, it could be a measure such as the range at which the device can detect a specified signal (system) level. Listed below are other ESM attributes that may be important in the threat description.

- Range to detection (specified signal)
- Target - Frequency hop/track ability
- Direction Finding accuracy and time requirements
- Frequency spectrum covered
- Decoding capability
- Line of Sight requirements

Electronic Countermeasures

ECM disruptive attributes center around the power the device can place in the system receiver. This power differs from the radiated power of the jammer by such factors as the bandwidth jammed compared to the receiver bandwidth. ECM deception, on the other hand, is effective to the degree that the adversary transmission mimics the authentic transmission and is accepted and acted on by the system.

- Effective Power (function of beamwidth, band width, radiated power)
- Frequency following capability
- Ability to mimic US transmissions
- Geometry between transmitter, receiver and jammer

3.6.2 Platforms

ESM and ECM platforms span the range of war vehicles. They include trucks, aircraft, helicopters, satellites, ships, submarines, and fixed ground sites.

3.6.3 Effects

The effect of ESM is critical information gained about the system of interest. This information can include the present and future location, identity, intentions, and command relations of the system. Thus the major effect is to make the system more vulnerable to further exploitation or future attack.

The effects of disruptive ECM are primarily to deny the system the use of various forms of electromagnetic energy. These forms can include navigation, communication, radar, and IR sensors. The overall effects can range from momentary confusion to substantial mission degradation, depending on the level and duration of disruption. The effects of deception vary widely and can make the system operators distrustful of sensors and messages.

3.6.4 Employment

The decision of where and how to employ EW is a complex one. Due to their high priority most strategic systems have an EW threat, if only ESM. In general, ESM and ECM are used in a complementary fashion. ESM collects targets for disruption and deception, while ECM may make ESM more effective by causing authentication schemes and radio discipline to break down. CONUS state-of-the-art C^3 systems are difficult to jam because of the poor jammer geometry and jam resistance of the waveforms. Space, aircraft and offshore ESM assets are still important, however. ICBMs in CONUS are vulnerable to EW mainly through their associated C^3 systems. Strategic aircraft can be vulnerable to the full range of EW, including communications ESM and jamming, disruption of external navigation aids, and deception.

3.7 CHEMICAL/BIOLOGICAL THREATS

Chemical and biological agents are mainly of concern in the tactical theatre, and are not as important for CONUS based strategic systems. This section is a quick overview of some of the salient features of the chemical threat.

3.7.1 Attributes

Chemical threat attributes include the following:

- Method of ingestion (skin, respiration, etc.)
- Effect on humans (percent lethality, incapacity)
- Time to affect humans
- Persistence (minutes to days)
- Delivery accuracy
- Delivery range
- Spreading method (wind, contact)
- Available resources (charges, delivery platforms)
- Ability to be detected by US sensors

3.7.2 Platforms

As with tactical nuclear and conventional weapons, chemical weapons can be delivered by a variety of platforms. These include:

- Tactical Aircraft
- Artillery
- Surface to Surface Missiles
- Multiple Rocket launchers
- Unconventional Warfare Teams

3.7.3 Effects

There are several major effects from the employment of chemical weapons. The first effect is loss of personnel or incapacitation, depending on the agent. This effect may occur in a very few minutes to a few hours. The second major effect of the use of chemical weapons is to force the recipient of the chemical attack to fight in Nuclear Biological Chemical (NBC) equipment. Establishing a chemical defense posture involves bulky, hot clothing, extensive decontamination, sealing buildings, and a general reduction in efficiency in operating equipment and performing procedures. The other major effects involve tactical considerations such as restricting use of terrain, channeling forces into specific areas, and delaying an ongoing operation (attack or defense).

3.7.4 Employment

Generally, strategic systems are most at risk to chemical weapons when deployed in theatres outside CONUS. The effectiveness of the lethality or incapacitation effects of chemical weapons is highly dependent on surprise. If the target is unprepared and not in a chemical defense posture, the agent can devastate a facility. If the target is prepared, inefficiency caused by NBC equipment will predominate. Operationally, chemical defense posture causes crew timeline delays, thus, posing a performance impact even if the weapons are ineffective.

3.8 DIRECTED ENERGY WEAPONS

Directed energy weapons are an evolving technology. DEW are not yet known to be fielded to destroy targets, but certain electro-optical devices can be used to blind personnel or sensors. Among the DEW of interest are lasers, high powered microwaves, (HPM) particle beams, and exotic hypervelocity kinetic energy weapons.

3.8.1 Attributes

Since this technology field is very new, there are few specific weapon attributes to list. Among those of concern to the analyst are:

- Energy deposited on the target (rate, total energy)
- Pointing accuracy (mils, CEP, etc.)
- Range in ambient medium (air, space)
- P_k vs Range

3.8.2 Platforms

Potentially, DEW can be hosted by many platforms including:

- Fixed ground sites
- Vehicles/ships
- Unmanned Satellites
- Space station platforms

3.8.3 Effects

The effects of DEW can be divided into four categories:

- Damage to humans including damage to eyesight
- Damage to sensors (IR, EO)
- Electrical damage to weapons system
- Mechanical damage to weapons system

The first two categories refer to tactical DEW like battlefield lasers and EOCM devices. The second two categories of damage are more often associated with strategic DEW. Electrical damage typically occurs at lower energy levels than mechanical effects.

3.8.4 Employment

Battlefield devices for the near future will focus on disruptive effects as opposed to destructive damage to the system. This is because of the transmission losses in the atmosphere and the lower power available from portable generators. Space and ground-based DEW may be able to cause destructive damage to the system as a whole. Space based US strategic assets are vulnerable to space-based adversary lasers, particle beams, and HPM, while ground based and air breathing strategic assets (bombers, C^3 nodes, cruise missiles) will primarily be vulnerable to HPM since the frequencies of microwaves appear to propagate well through the atmosphere.

3.9 TYPICAL THREAT TREES

This section summarizes the generic threats discussed in the last several sections to three types of strategic systems: ICBMs, strategic aircraft, and C^3 systems. "Threat trees" that divide the specific threats into the classes discussed above are used to describe each category of system threat.

3.9.1 ICBM System

Figure 3-5 contains the threat tree for a generic ICBM system. The threat description that goes along with this tree would include most of the aspects of the threat

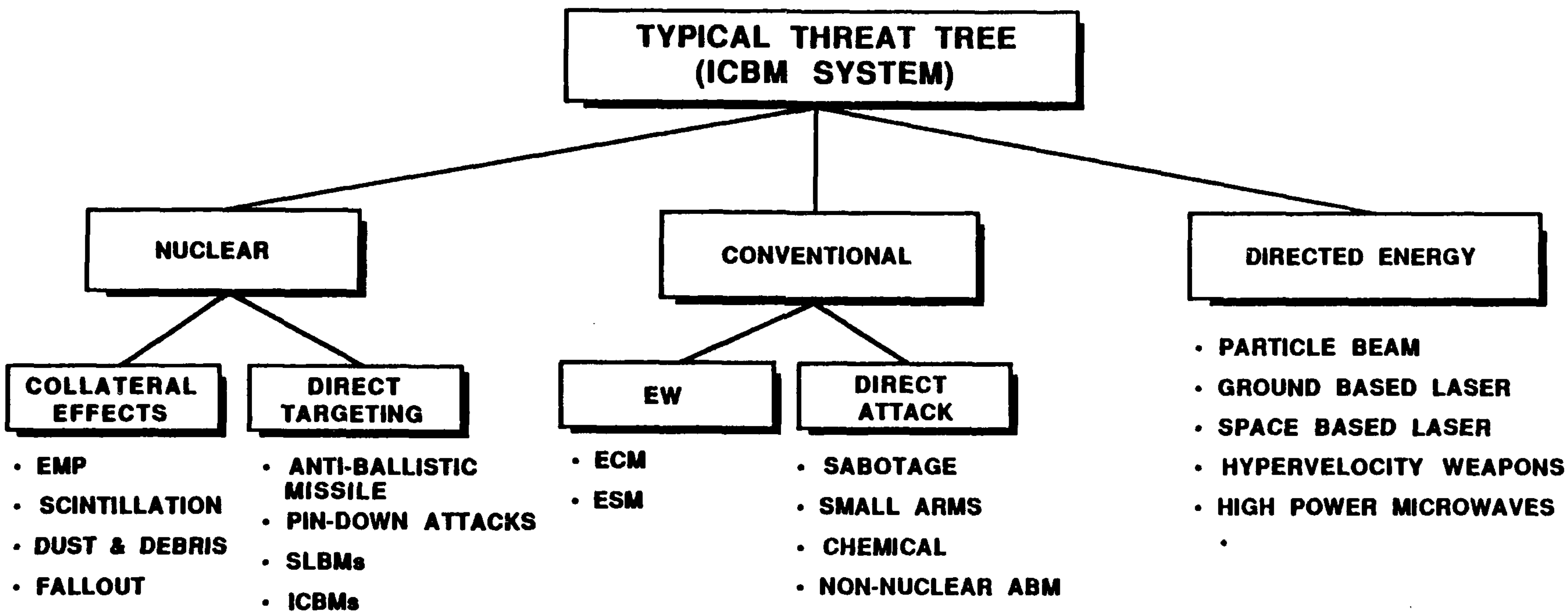


Figure 3-5: Threat Tree For ICBM.

classes described above. As might be expected, the majority of the tree is devoted to nuclear threats to the system.

3.9.2 Strategic Aircraft System

Figure 3-6 is the threat tree for a strategic aircraft. The nuclear threat is mostly composed of collateral effects, since it is presumably difficult to directly target an airborne aircraft. The tree also contains a significant conventional threat to cover the exposure of the system to adversary homeland defenses, or tactical air defenses in the bomber's tactical role.

3.9.3 C^3 System

Figure 3-7, the threat tree for a C^3 system, again has a significant nuclear threat, as well as an expanded EW threat. The C^3 system has elements of space (presumably) and fixed ground sites threats.

3.10 Threat Description for SLINK System

We continue our SLINK system example in this section, by briefly outlining the threat classes and attributes that apply to the system. We follow the outline of this chapter to develop the threats.

The SLINK system is located about 100 km behind the FLOT (Forward Line of Own Troops) in the theatre of war. As such, it is susceptible to the entire range of conventional threats, as well as chemical threats. Being a strategic C^3 system, it is of high value in a strategic conflict, and therefore is a target of nuclear weapons, should the conflict escalate to that point. Finally, being a communication system, the emissions make it a target of direction finding electronic warfare, as well as a priority target for jamming. In fact, the only threats not strongly applicable to the SLINK are strategic nuclear weapons, and directed energy weapons. Strategic nuclear weapons are not generally used in theatre (except for possible High Altitude EMP or comm disruption bursts), while directed energy weapons are not well suited to attacking ground targets in the rear of the enemy. Let us assume that intelligence has made a potential case for a space-based microwave communications disruption weapon, but with a low likelihood of such a weapon being developed in the life of the SLINK. Figure 3-8 is a pictorial representation of the threats to the SLINK system. These threats are developed in more detail below.

So, there are three characteristics of the SLINK that lend themselves to being attacked. First, it is in a theatre of conventional war. Second, it is a strategic

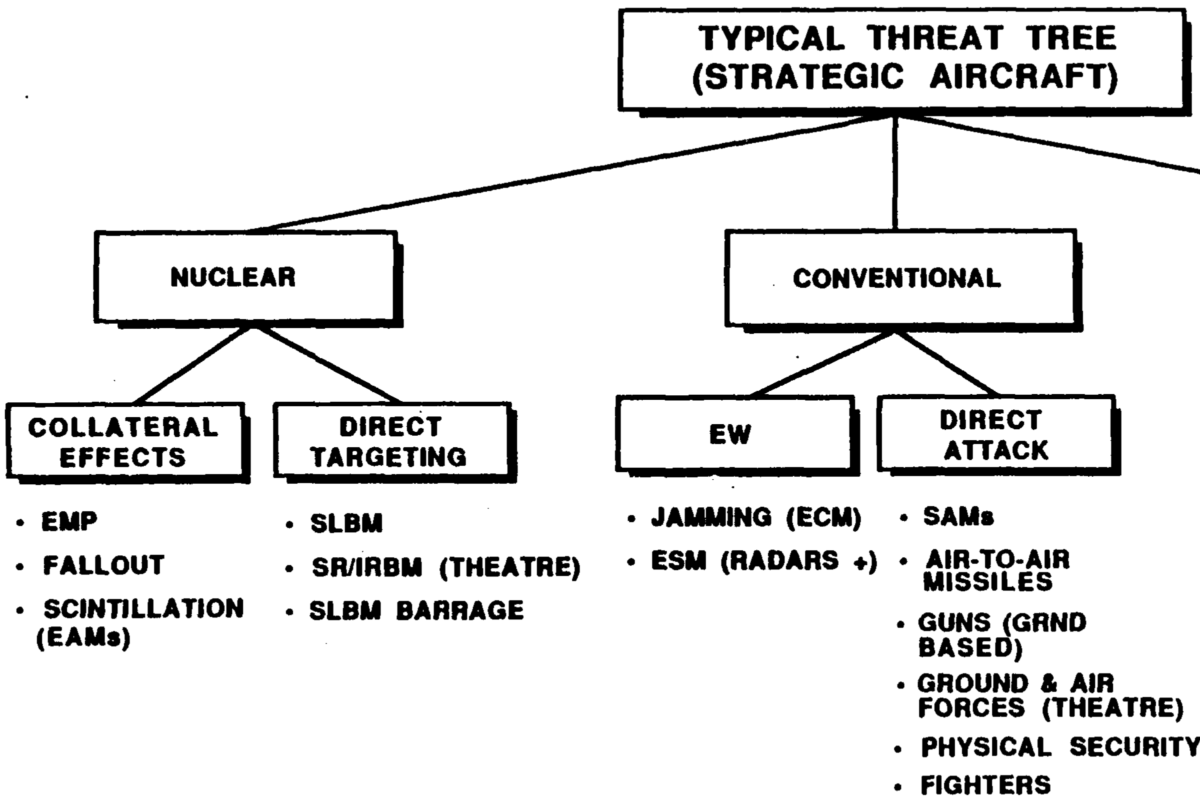


Figure 3-6: Threat Tree For Strategic Bomber

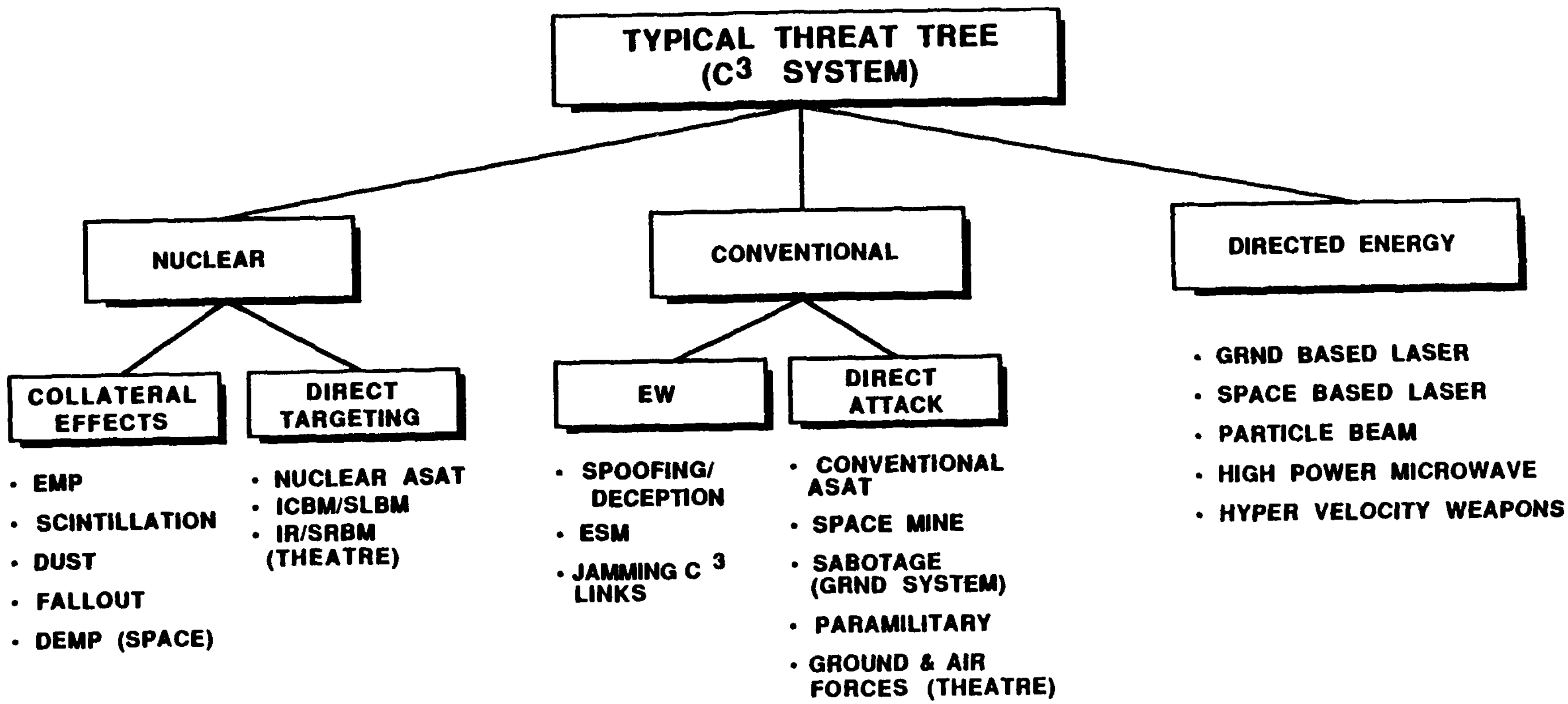


Figure 3-7: Threat Tree For C^3 System

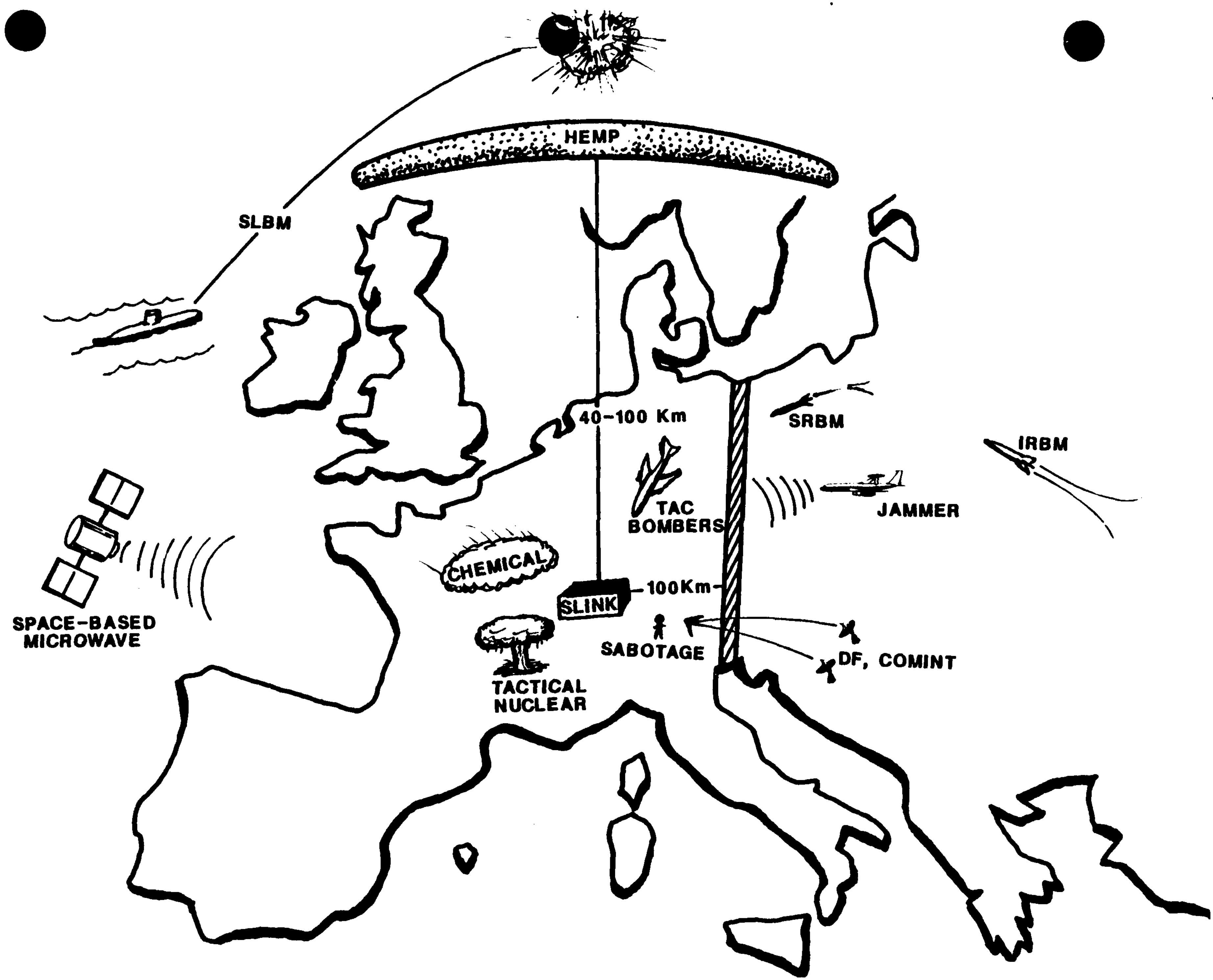


Figure 3-8: SLINK Threat Pictorial

command and control asset, making it a priority target. Third, it is a communications asset, leaving it susceptible to EW. The table in Figure 3-9 shows the principal threats to the SLINK system. The table lists the category and subcategory of threat, some of the threat attributes mentioned in this chapter, the delivery platforms for the threat, the principal effects of the threat weapons, and a few comments on the employment of the threat.

The nuclear threat to SLINK consists primarily of direct attack by tactical nuclear weapons and high altitude EMP or communications disruption detonations. The direct attack by tactical nuclear weapons will necessarily be by platforms with the range to reach 100 km behind the lines. This limits the platforms to tactical aircraft, and certain missile types. The major effects from tactical nuclear weapons of low yield are blast, thermal pulse, and possible gamma or neutron radiation. The adversary places HQ communication assets number two on his nuclear targeting list, making SLINK a likely target if the conflict escalates. The high altitude bursts will affect systems theatre wide -- including the adversary's systems. It is therefore problematical whether the adversary would risk damage to his own systems by making a HEMP attack on the SLINK. For purposes of further explanation, we will not eliminate HEMP as a potential effect.

OT&E should always consider the crew of the system. With that concept in mind, long-term radiation exposure of the crew in the nuclear battlefield will also be a threat to the system. If SLINK is to survive to provide enduring communications beyond a period of a few days, the total dose of radiation to the crew may exceed the lethal or incapacitating levels. Due to the complexity of this subject, it will not be considered in more detail in this pamphlet, but an actual operational scenario for SLINK would be incomplete without it.

Since SLINK is mobile and is located 100 km behind the battle lines, conventional ground forces will not be a major threat to the system. However, tactical air and surface to surface missiles can reach the SLINK sites. In addition, there is the sabotage threat posed by small groups of specially trained soldiers. For both threats, the effects are similar -- the destruction of equipment and the loss of personnel. As mentioned above, HQ C^3 facilities are priority targets for the adversary, especially in theatre.

Electronic warfare threats to SLINK are two: ESM and ECM. The ESM threat is crucial since direction finding equipment that locates the hidden, mobile SLINK makes the

CATEGORY	SUBCATEGORY	ATTRIBUTE	PLATFORMS	EFFECTS	EMPLOYMENT
NUCLEAR	TACTICAL	• 1-100 kT 60-500Km 30-300 mCEP AIRBURST	• TACTICAL AIRCRAFT CRUISE MISSILE IRBM SRBM	• BLAST THERMAL RADIATION	• HIGH PRIORITY REAR (60Km+) TARGET. EARLY TARGET WHEN CONFLICT ESCALATES. SOFT TARGET
	STRATEGIC	• 1MT, 40Km*ALTITUDE	• SLBM	• HEMP	• HEMP BURST POSSIBLE
CONVENTIONAL	ARMY/AF	• 500-1000 LB HE GRAVITY BOMBS 100-300 FT CEP	• TACTICAL AIRCRAFT 300 MI RANGE SRBM	• BLAST FRAGMENTS	• PRIORITY AIR C3CM TARGET
	SABOTAGE	• 2-10 PERSON TEAMS AUTO WEAPONS EXPLOSIVES	• FOOT AIRBORNE CIVILIAN VEHICLES	• BLAST FRAGMENTS SABOTAGE EQUIPMENT	• COVERT MOBILE FORCES SURPRISE AND SPEED
	TERRORISM	• UNLIKELY			
ELECTRONIC WARFARE	ESM	• HF-EHF DF VEHICLES + INTERCEPT - COMINT IR, RADAR AEROSPACE SENSORS	• TRUCK, VAN, AIRCRAFT SATELLITE	• LOCATION, EXPLOITATION	• LOCATE EQUIPMENT IN PROPER GEOMETRY. LOCATE SLINK & LISTEN
	ECM	• INTRUSION, DECEPTION, BARRAGE FOLLOWER JAMMERS 10-1000 W	• TRUCK, VAN, AIRCRAFT SATELLITE	• COMM DENIAL, DELAY CONFUSION, MISDIRECTION	• MIMIC, JAM OR BOTH IN COMBO WITH ESM
CHEMICAL	PERSISTENT/ LETHAL	• NERVE, BLOOD AGENTS MINUTES TO DEATH 10-48 HR PERSISTENCE	• TACTICAL AIRCRAFT SRBM	• DEATH • INEFFICIENT OPERATIONS IN CHEM DEFENSE GEAR	• REMOVE SITE FROM ACTION AND DENY AREA TO US SURPRISE IMPORTANT
DIRECTED ENERGY	BATTLEFIELD LASER	• UNLIKELY - LINE OF SIGHT			
	SPACE-BASED MICROWAVE	• LOW EARTH ORBIT (100's MI) 90 MINUTE PASS, 10 Kw POWER	• SATELLITE	• ELECTRONIC DAMAGE FROM TRANSIENT CURRENTS & VOLTAGES	• SINGLE PASS, SHORT ENGAGEMENT (<1 MIN)

Figure 3-9: SLINK Threat Description Table

site a target for all other threat types. Without the ability to find SLINK the adversary cannot attack it. The other form of ESM that may be important is the intercept and exploit threat. If the adversary can learn of US strategic intentions, including resupply times, conflict escalation to nuclear or chemical weapons, and overall strategies, they will be immeasurably helped.

The ECM threats include jamming and deception. Both can seriously reduce the effectiveness of the SLINK system by causing confusion and delay. Both types of EW threats can be mounted on many platforms, and may be effective at extended ranges.

A chemical attack on SLINK would rely on surprise and speed to catch the system unprepared. Presumably, since SLINK is a priority target, it would be among the first to suffer chemical attacks. The adversary's intent would be to permanently remove the system from operation, and since the SLINK is a rear target, persistence of the agents would pose the adversary few problems. So, the most likely attack would be persistent lethal agents to incapacitate the SLINK personnel and deny the area to reinforcements or replacement crews.

The potential microwave satellite threat would be most effective against the deployed SLINK antenna and equipment vans. Microwaves rely on exciting transient voltages and currents to damage the target. The likely platform would be a low earth orbit satellite, making a pass over the SLINK about every 90 minutes. The engagement would consist of one or a few high energy pulses of microwave energy. Note that the microwave threat is currently considered less likely by intelligence agencies to be deployed and has a low likelihood during the life of the SLINK.

We have described the mission of the SLINK (Section 2), and have just completed an outline of the threat description for the system. When these two are folded together and refined, they comprise the operational scenario -- the subject of Section 4.

4.0 DEVELOPING AND REFINING THE OPERATIONAL SCENARIO

4.1 INTRODUCTION

At this point, the analyst has a preliminary description of the system mission along with the major mission functions and the mission timeline. The analyst has also compiled a description of all important threats to the system. These two steps are now going to be molded together to produce the operational scenario. Figure 4-1 shows where we are in this process. As in all steps in this process, the level of detail depends on the needs of the OT&E program and the data available. The threat scenario may be as brief as a few pages of text and matrices, or a complex 50 page document. We should stress here that the analyst is not in this process alone. In the previous two steps, he/she has had help from the system designer, intelligence agencies, the system user, and support organizations within AFOTEC. These same contacts and sources should now be exploited to complete the scenario.

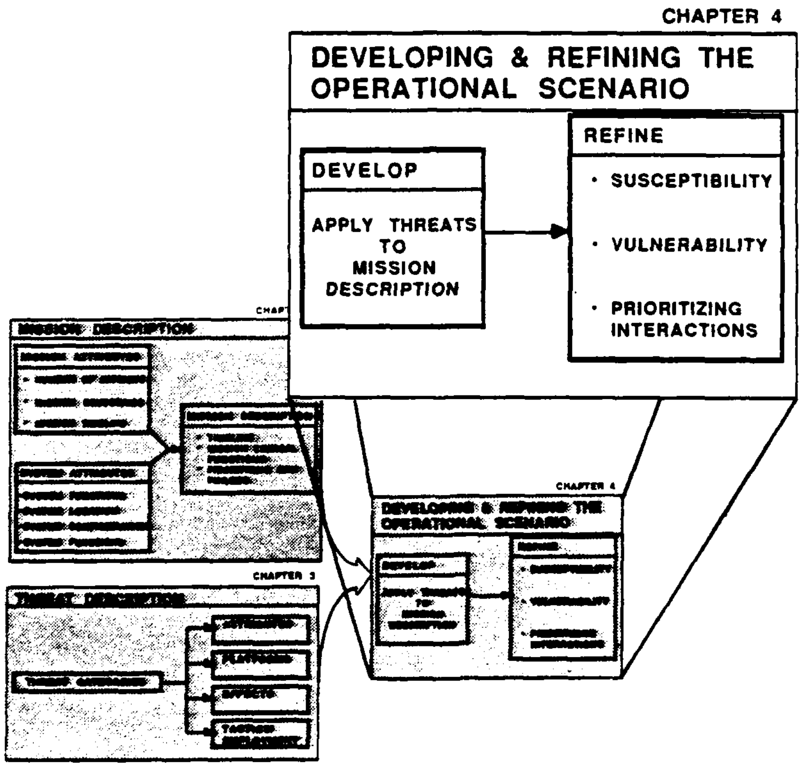


Figure 4-1. Operational Scenario Development Process (Scenario Refinement)

In brief, the operational scenario is composed of the system mission description and timeline with the threat overlaid. The threat is applied to mission phases (if applicable) and mission functions that occur during the phases by applying threat attributes (effects, timing, accuracy) to system attributes. The scenario is then refined as described in Section 4.5.

As mentioned in the previous sections, neither of the first two steps in the process -- the mission description or the threat description, -- were developed without an appreciation for the other. In developing the mission description, the analyst had in the back of his mind an idea of the major threats faced by the system. In choosing the threats to be included in the threat description, the analyst considered the system and mission the threat could be applied to. Therefore, he already has the basis for the first activity in the final step in this process. This activity is the initial application of the threat to the mission description. This initial application will be refined into the final operational scenario(s).

Once the threat has been applied to the mission, the operational scenario is refined by considering the priority of the mission functions, the susceptibility and vulnerability of the system to the threat.

This section begins as the other sections have done, with a set of data sources the analyst might refer to, and continues with a set of guiding principles. The section concludes with a detailed description of the process and examples of how the process can be applied.

4.2 DATA SOURCES

In developing the final operational scenario, the analyst is really deciding how the war might be fought effectively against the system under test. Therefore, this section is more highly dependent on an understanding of the art of warfare than the previous two steps. Since analysts come to AFOTEC from a variety of operational and staff backgrounds, some of the readings suggested below may not be applicable. However, the reading list is intended to include selections that may prove useful to refresh the analyst's memory of principles and applications of weapons. Most of these references are available in the AFWL Base Library. The classified references can be ordered from the responsible organization. Regulations and manuals can be obtained through AFOTEC/DA.

General Strategy

On War, Carl Von Clasuwitz
The Art of War, Sun-Tzu
Strategy, Liddell Hart
Strategy in the Missile Age, Bernard Brodie
The Command of the Air, Guilio Douhet

US Doctrine and Strategy

JCM 1-1
AFM 1-1, Doctrine and Strategy
US Army FM 100-5, Operations
JCS Posture Statement (Secret -- yearly)
JCS Strategic Capabilities Study. (Top Secret -- yearly)

Soviet Strategic Thought and Weapons Inventory

Soviet Military Power, DoD (yearly)
Annual Soviet Military Power Issue, AFA Magazine
Whence The Threat to Peace Soviet Counterpart to Soviet Military Power
SDIO Threat Document, SDIO (Secret)

Soviet Tactical Operations

Anti-Satellite Weapons, Countermeasures and Arms Control, OTA, September, 1985
Opposing Forces, Europe, USA FM 30-102
TACM 3-1, TAC/DO
Analysis of Chemical Warfare Operations IDA P1812, 1985

Miscellaneous Reading

Air Force Physical Security Program
USAF Anti-Terrorism Program
The Third World War, General Sir John Hackett

4.3 GENERAL PRINCIPLES

4.3.1 Conservatism

Conservatism is the rule in defining the operational scenario at the early stages of OT&E. The intent of the operational scenario is not to extensively study the threat and mission and reduce the multitude available to only a few threats that definitely will affect the system. Instead, the operational scenario removes only those threats that almost surely will not affect the system in a major systematic way. The detailed analysis of the scenario to quantify the survivability of the system is the task of the OT&E itself -- not the plan or approach. For example, the SLINK threat description includes a potential SRBM as a conventional threat. If the SLINK system is lightly armored, the adversary may not have a missile accurate enough to pose a serious threat to the SLINK. However, that accuracy and hardness analysis is left to the OT&E itself and is not a part of the threat scenario. Therefore, the analyst should approach this final step considering how to prioritize the threat to the system and mission, and remove only those threats in the threat description that, in his judgement, need no further study.

4.3.2 Geography

The physical location of the threat and the system during the mission is certainly a prime factor in deciding how the threat will be applied. The analyst should not, without good reason, arbitrarily locate a threat within striking range where none has existed or would be appropriate. For strategic systems, this includes placing SAMs off the coast to attack bombers, postulating hidden CONUS jammers, or landing sizeable ground forces to attack an ICBM installation. Using commands often have adversary order of battle information that can help position each major adversary threat system.

4.3.3 Resources

The analyst should have a general understanding of the competing battlefield uses for adversary resources. For example, if the adversary has only a few hundred SLBM warheads of a particular yield and accuracy, the adversary would not commit his entire force to attack a mobile airborne command post with uncertain success. The warheads would be better used servicing classic SLBM targets. This principle is not to suggest that the analyst must conduct extensive cost-benefit studies, but he/she should keep in mind that the adversary is resource limited (as we are) and has many other attractive targets to attack. User studies groups like the SAC Office of Scientific Research (SAC/NR, Mr O'Meara or Mr. Stamm AV271-2763) have often conducted these kinds of cost-benefit studies and can estimate the adversary's priorities for using his weapons.

4.3.4 Level of Conflict

The threat to strategic systems varies with the level of conflict. ICBM threats can generally be covered with a single general nuclear warfare scenario. C^3 systems have two potential scenarios that could be written. The first of these is an ESM and jamming threat that varies directly with the level of conflict, from day-to-day tensions to general nuclear war. The second scenario includes nuclear weapons effects in theatre or general nuclear war, as well as the EW threat. Strategic aircraft could require several scenarios as a consequence of their multiple roles. Strategic aircraft scenarios include conventional war, theatre nuclear war, and general nuclear war. The point of this principle is that the analyst must consider the levels and theatres of conflict before deciding on using one or several scenarios for the system.

4.3.5 Crew In the Loop

One crucial difference between operational and developmental testing is that OT&E specifically is tasked to consider the operator of the equipment. For the operational scenario, and survivability in general, this means that the analyst must consider the effect of the weapons on the humans that crew the system. The analyst must also consider the crew responses to unusual system behavior. The weapon effects can include:

- burns
- flashblindness
- skin blistering
- eye damage
- nausea (chemically induced) and radiation sickness (prompt and chronic)
- bruises, contusions, and broken limbs
- deafness
- death
- confusion and delay in operator/system interaction
- increased operator workload
- errors and missed actions

When developing the operational scenario, the analyst must always consider that the human is a vital part of the system, and that some weapon effects can incapacitate the crew while leaving the equipment relatively unscathed or produce operator interface problems especially in software intensive systems. So, while developing the scenario, and after, the analyst should review it to determine if the threats to the system include those that principally threaten humans.

4.4 INITIAL APPLICATION OF THE THREAT

The initial application of the threat to the mission is a fairly straightforward process. It can be done in several formats. The idea is to consider each mission phase in the timeline and decide which threats can engage the system. The analyst should not be too exclusive at this point, but simply lay out all the physically possible threat-system interactions.

This application can be done in matrix form, listing the mission phases or time periods in one column, and the possible threats in the rows. Figure 4-2 is an example of

THREAT / MSN PHASE	ALERT/ TAKEOFF	CRUISE/ REFUEL	PENETRATION	RECOVERY
HEMP	X	X		
SLBM DIRECT	X	X		
SLBM BARRAGE	X	X		
NAVAL SAM			X	
AI-CONV			X	X
AI-NUCLEAR			X	X
RADAR JX			X	X
COMM JX	X	X	X	X

Figure 4-2: Initial Application of Threat to Strategic Bomber (Matrix)

the matrix format applying threats to the strategic bomber mission. The threats to the bomber (rows) range from nuclear attacks on the base to airborne interceptors (AI) during the penetration of the adversary territory. The four major mission phases are self-explanatory. The "X"s in the table indicate where the threats are likely to attack the system. The blanks represent unlikely threats during that mission phase. For example, the blank in the HEMP/PENETRATION cell means that the adversary would be unlikely to detonate a HEMP weapon over his own territory on the possibility that it might damage his own systems in addition to the targeted bomber. Blank threat/mission phase cells indicate that the combination will no longer be considered in the scenario.

An alternate representation of the initial application is in the timeline format. Figure 4-3 shows similar threats to a strategic bomber over time. This representation includes the window of opportunity for each of the mission phases by including the duration of the phase. It also includes the altitude/distance of the bomber in the flight profile.

4.5 REFINING THE SCENARIO

In this activity, the analyst refines the scenario by considering the susceptibility of the system to the threat, and the vulnerability to the threat. The analyst is not required to do extensive technical studies here, but only to screen out those threats that are not major factors in the survivability of the system. The technical studies are the subject of the OT&E execution -- not the planning process. The analyst should document his reasoning for deleting any threat during this activity. The documentation of the analyst's reasoning will be important in the final activity of the process: prioritizing the threats and functions. The prioritization process is described later in this section.

Describing how to refine the operational scenario is difficult to do generically, since the susceptibility and vulnerability factors for each system will be unique. Indeed, that is often why a new system is developed -- to reduce susceptibility or vulnerability. So, this activity will be described with examples and questions for the analyst to consider.

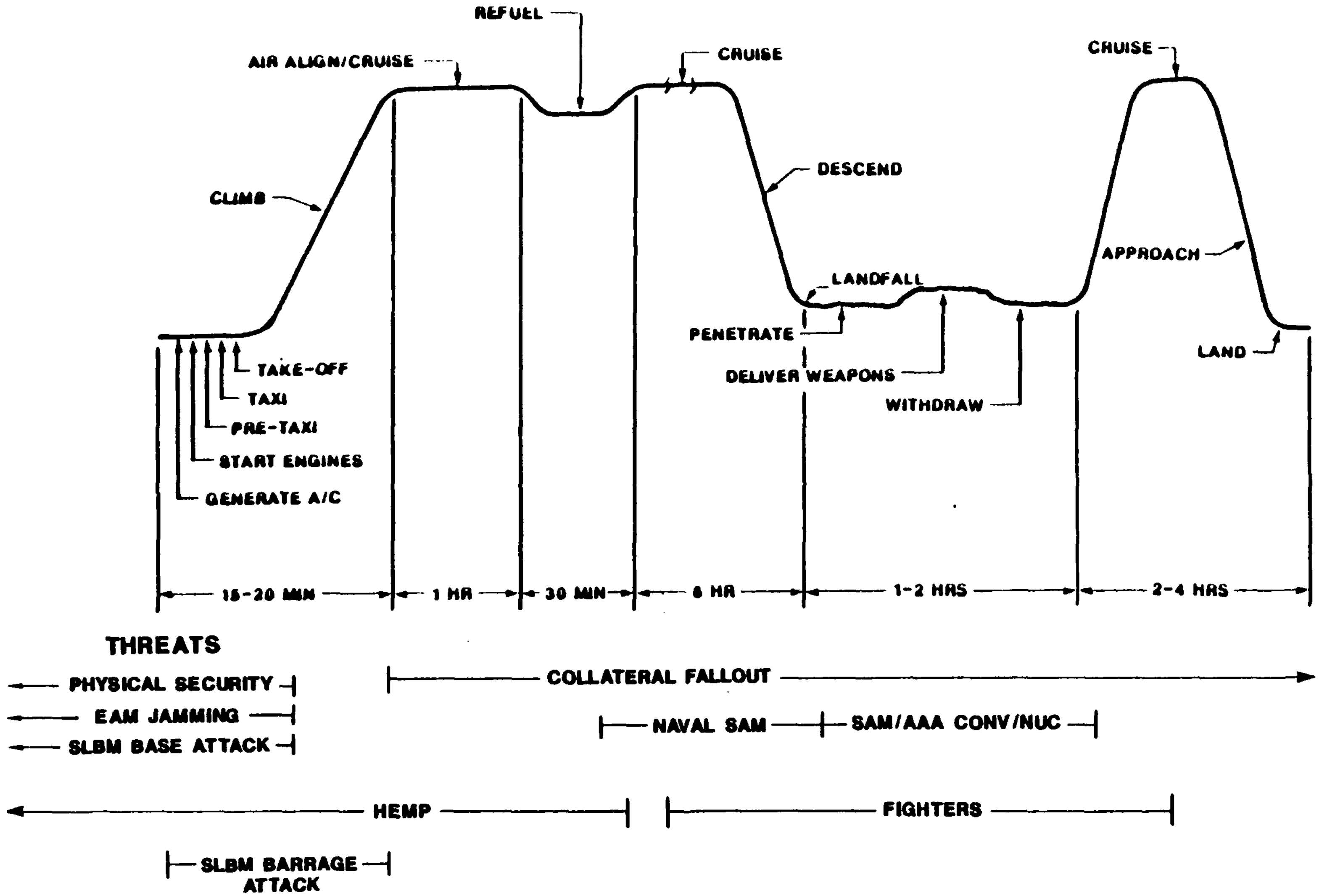


Figure 4-3: Initial Application of Threats to Bomber Threat (Timeline)

4.5.1 Susceptibility Analysis

The question of whether a system is susceptible to a threat is to ask if the threat can detect and engage the system. Susceptibility is defined as the combination of factors that allow a system to be engaged by an adversary threat. It includes such factors as:

- signatures and observables
- agility/maneuverability
- decoys/deception
- countermeasures
- warning
- threat suppression
- proliferation
- tactics

To screen out threats on the basis of susceptibility factors, the analyst should ask himself questions of this sort:

Is it <u>possible</u> for the adversary to:

- detect the system or system signatures?
- locate the system, identify it and decide to target it?
- have time to detect and engage the system while it is exposed?
- position a threat to physically engage the system?
- protect his threats from suppression attempts?
- keep from being confused by deceptive techniques?
- economically target the system considering
  - -- decoys?
  - -- other uses for the resources?
  - -- deception or mobility techniques?
  - -- probability of kill?

If all these things are <u>possible</u> then the system can be said to be susceptible to the threat. The threat should be kept in the operational scenario.

To illustrate this process, take the SLINK system we have been examining, and only two of the threats contained in the threat description: IRBMs and jammers.

The analyst might reason along these lines. The site is mobile and presumably unknown to the adversary. Therefore, the adversary could target the system if they can find it through ESM devices. SLINK is an important communications center and therefore the adversary would consider the center a priority target. There are significant decoys and deceptive measures in place to confuse the adversary targeting capability. Therefore, there is some question as to whether the adversary can effectively target the system -- that is, SLINK may not be very susceptible. However, we cannot rule out IRBMs on the basis of this reasoning, and more detailed studies will be necessary in the actual conduct of the OT&E. IRBMs stay in the scenario. The question of the effectiveness of such an attack is addressed when the example is continued in the next section under the vulnerability of the center.

For jamming, assume the SLINK communicates via a combination of highly directional radio line of sight and satellite relays, and the SLINK is located well behind the lines of battle in the theatre. In this case, it may be quite difficult for an adversary jammer to position itself between the transmitter and receiver. Depending on the intelligence assessment, a portable jammer carried by an unconventional warfare team might be a remote possibility. So, the SLINK is not very susceptible to jamming, except for the unlikely unconventional warfare case. However, we cannot rule out the possibility that a high powered adversary jammer could direct energy into even the highly directional SLINK antenna. We must therefore retain the jammer in the scenario, but at a lower priority.

4.5.2 Vulnerability Analysis

The question of vulnerability is perhaps more difficult to answer in this general way than that of susceptibility. Vulnerability is defined as the extent of degradation to the system functions as a result of being successfully engaged by a threat. These degradations range from momentary confusion (jamming, deception) to catastrophic loss of the system (nuclear weapon).

Vulnerability factors include:

- damage tolerance in the system
- armoring or shielding
- redundancy of components or elements
- protection of the crew
- combat damage repair
- threat circumvention
- damage control/isolation measures

Vulnerability reduction allows a system to keep on operating at, or near, designed efficiency despite being engaged by a threat.

Vulnerability data is generally supplied by the DT&E test program, with appropriate operational inputs from OT&E. It is dangerous for the operational tester to make vulnerability assumptions in the absence of test data to support them.

In no case should the operational analyst screen out a threat because some design feature presumably makes the system invulnerable to a weapon effect. Verifying the design performance of the system is the task of the developer. In some cases, the system will not operate as designed, and it is the task of the operational tester to evaluate the effectiveness of the system as it actually works in its intended operational environment. To dismiss a threat to the system because the system has been designed as invulnerable to that threat, before that level of vulnerability has been demonstrated by the developer, is to diminish the responsibility of OT&E.

Vulnerability screening is a more difficult chore since the analyst will have to consider weapons effects physics, the interaction of the effect with the system, and the final impact on the system functions. Accordingly, this screening process should be even more general and conservative than the susceptibility screen. As a general rule, the analyst might consider downgrading the priority of a threat based on vulnerability, but should not delete a threat simply on that basis. In summary, the susceptibility screen can delete threats, but the vulnerability screen primarily makes the threat a lower priority.

The analyst should consider the threat effects first, followed by the system design features, and finally the impact on the system functions.

Weapon Effects: Are the effects:

- due to direct or collateral targeting?
- prompt, delayed or cumulative?
- primarily directed against electronics, mechanical devices, or the crew?
- directed against the system exterior or interior?
- degrading or destructive to the system?
- widespread or local?
- manifested immediately or later?
- restricted to a particular engagement geometry?
- fatal to the crew or equipment first?

System Equipment and Functions Interaction

Is the system:

- designed with redundancy in equipment?
- shielded from weapons effects?
- electrically or mechanically responsive to the threat?

By asking these questions (and answering them) the analyst gains insight into the effect of an engagement on the system. To illustrate a few of these principles, the SLINK system example is continued.

The SLINK vans might not be hardened to blast and thermal effects to any significant degree, so the adversary has good confidence that an attack would be effective. The facility is hardened to HEMP, so the adversary would not wish to rely on the HEMP burst to negate the facility. This lack of vulnerability to HEMP encourages the adversary to attack the facility directly. The last point made here illustrates the cyclical relation between vulnerability and susceptibility, and the importance of an integrated threat scenario. Although the facility is susceptible (can be exposed) to HEMP, it may not be vulnerable (will not be affected). Therefore, SLINK's HEMP hardening makes direct attack of the system a very desirable option.

The HEMP threat has another interesting aspect. So far, we have discussed the threats to SLINK in isolation -- not considering the collateral effects on SLINK of attacks on other systems. There are many tactical systems in the theater that are not hardened to HEMP. Therefore the adversary may use a high altitude EMP attack against these systems. So, while this HEMP burst would not be primarily intended to damage SLINK, SLINK will experience the effects of the burst intended for other systems. However, as mentioned previously, a HEMP attack will also affect the adversary's theater systems. In deciding whether to include HEMP, we must consider susceptibility (high), vulnerability (low), and threat likelihood (medium). Although this threat can be argued several ways, we will include HEMP in the scenario, but at a lower priority.

4.5.3 Prioritizing the Threats/System Interactions

The final activity in refining the operational scenario is prioritizing the threat/system interactions according to the three factors considered so far:

- criticality of mission function (Chapter 2)
- susceptibility -- likely to encounter
- vulnerability -- major system degradation

The highest priority threat/system interaction would be the one that affects the most critical mission functions, that the system is most susceptible to, and the system is most vulnerable to. For example, radiation from fallout is a threat that will be experienced by almost all CONUS systems that survive a general nuclear exchange (all are susceptible). If a system's data storage function is highly critical, and the data storage medium is highly vulnerable to nuclear radiation, then fallout would be a high priority threat for that system.

So, to perform this prioritizing activity, the analyst considers these three factors in either a qualitative and subjective way, or using some quantitative ranking method. Figure 4-4 is a repeat of the threat/system interaction matrix for a strategic bomber. Each cell marked with numbers represents a location in the mission timeline that a threat could engage and affect the system. The mission functions have already been ranked in the mission description phase ("M" numbers). The analyst also has in hand his descriptions of the susceptibility and vulnerability of the system to each threat from the refinement steps above.

If the analyst wishes to subjectively rank the threats, he/she can simply trace through the matrix, assigning a '1' to the cell he/she judges to be most important, a '2' to the next cell, and so on. Or, the analyst can assign three numbers to each cell on a scale of 1 to 10. One number stands for mission phase/function criticality, one for the susceptibility of the system to the threat in that mission phase, and one number for the vulnerability of the system to that threat during that mission phase. The weighted, or unweighted average of the cell numbers can be used to rank the interactions. Refer to the AFOTEC/OA Technical Paper #9, Service Report Prioritization, for additional methods of ranking cells.

These rankings can be used to determine the relative amount of OT&E effort to be expended on the particular threat/system interactions in the operational scenario. They can also be used to justify the method of evaluation in the survivability test plan section, or to influence the DT&E survivability test program. For example, in Figure 4-4 we would have placed the HEMP attack on the base as a first priority, followed by the SLBM direct attack on the base, followed by the nuclear AI threat during penetration. The OT&E would have to take these priorities into account in deciding what resources would be devoted to system field tests of HEMP, to a digital model of the SLBM attack, and to component testing to resist the effects of the air-to-air missile nuclear warhead. These priorities give the OT&E team ammunition to approach the SPO with requests for information from DT&E tests, and for requests to modify the tests to include OT&E requirements.

4.6 ADDITIONAL CONSIDERATIONS

To complete the operational scenario, the analyst should document the entire process. A Survivability Architecture Plan/Briefing is frequently used to summarize the results. The importance of survivability in the system OT&E, the stage in the OT&E process, and the use of the scenario will determine how the scenario should be documented. A suggested outline is contained in Annex B.

THREAT \ MSN PHASE	M-3 ALERT/ TAKEOFF		M-2 CRUISE/ REFUEL		M-4 PENETRATION		M-1 RECOVERY	
	S	V	S	V	S	V	S	V
HEMP	10	6	10	9	1	7	1	2
SLBM DIRECT	10	10	3	7	-	-	-	-
SLBM BARRAGE	6	9	5	7	-	-	-	-
NAVAL SAM	-	-	-	-	7	7	-	-
AI-NUCLEAR	-	-	-	-	9	7	3	7
RADAR JX	-	-	-	-	4	2	2	1
COMM JX	4	10	5	8	10	2	2	2

S - SUSCEPTIBILITY RANKING (1 = LOWEST)

V - VULNERABILITY RANKING (1 = LOWEST)

M - MISSION PHASE CRITICALITY (1 = LOWEST)

Figure 4-4: Prioritizing Threat/System Interactions (Strategic Bomber)

The analyst may also, depending on the system, desire to include environmental factors like weather, humidity, temperature, etc. in the threat description, if these influence the performance of the system with respect to the threat, or the effectiveness of the threat. Terrain types may also be included, if the system is designed to use terrain masking (e.g. bomber) as a means of avoiding the threat systems. For communication systems, descriptions of the expected atmospheric noise, scintillation, or other factors may also be included.

If the analyst expects that detailed threat/system digital modeling will be required in the OT&E, he/she may wish to include the available information on logistics aspects of adversary weapons, operator reaction timelines, etc. These will certainly be filled out in the test execution phase, but including them in the operational scenario may save time later in the test. Resupply times, employment doctrine, supply caches, and other factors may also influence the scenario and can be included if available.

4.7 CONCLUSION OF SLINK OPERATIONAL SCENARIO

This section will illustrate the final steps in the SLINK operational scenario. We will apply the threat to the mission timeline and prioritize the threats and mission phases.

4.7.1 Initial Application of the Threat

Figure 4-5 is a repeat of the SLINK operational scenario outline from Section 1. It shows the scenario as it stands after the intial application of the threat to the system mission. Note that no threats have yet been deleted. The communications jamming threat is active only during those times the SLINK is transmitting. Similarly, the adversary must re-locate the SLINK each time the system moves. If they cannot locate the SLINK, then the system is not susceptible to further attack. Nuclear and chemical attacks do not occur until the conflict escalates to that point. Sabotage, on the other hand, occurs from the start of, or even slightly before, the actual conflict.

4.7.2 Refining the Scenario

The threat: have been applied to the SLINK timeline; now we will see if it is feasible to rank some segments of the mission or some threats, as more important than others. For example, the high power microwave satellite is listed by intelligence as a remote possibility during the SLINK lifetime. If this estimate continues, it may not be wise to spend too much time closely examining the vulnerability of SLINK to a marginally possible system.

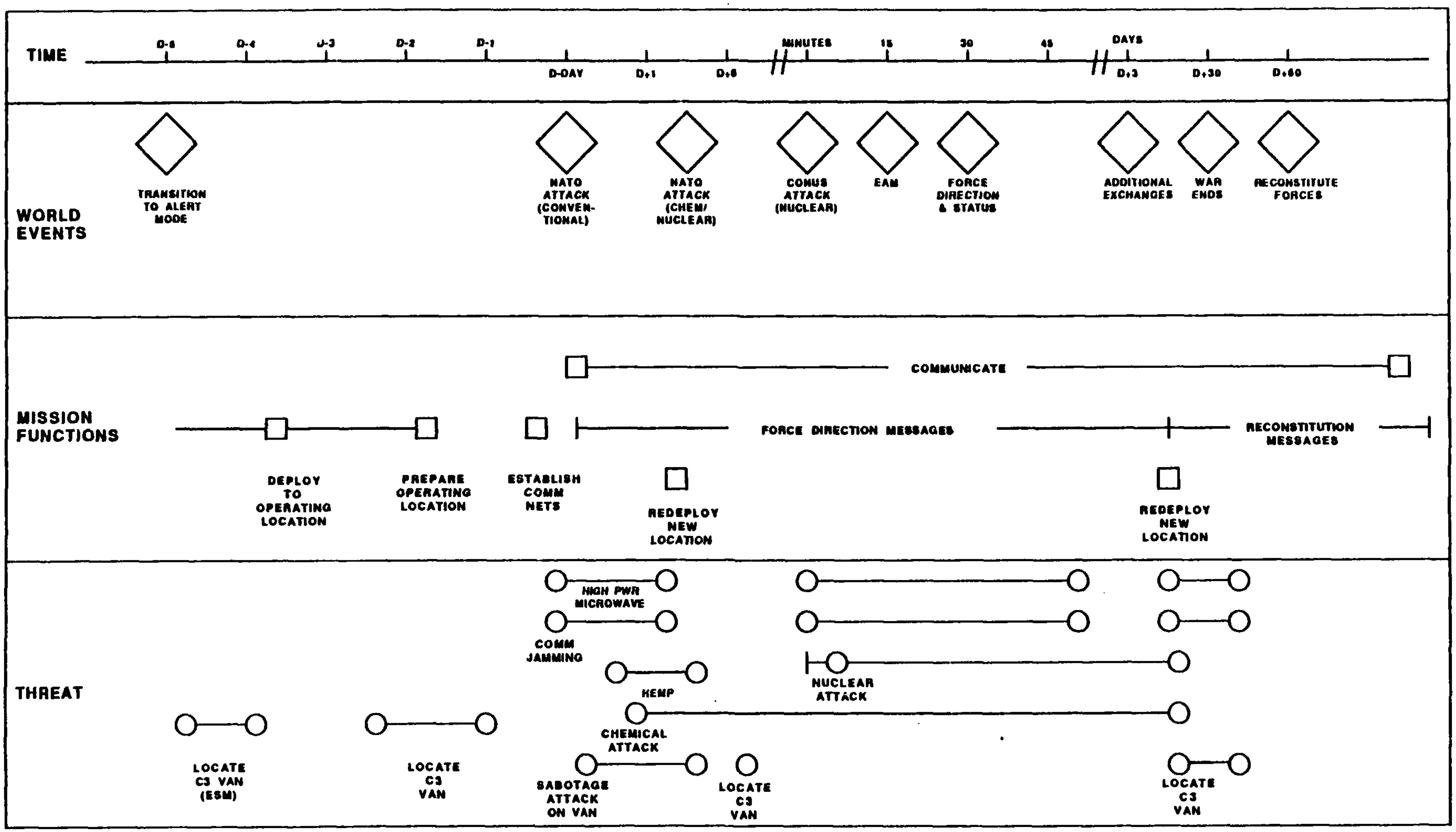


Figure 4-5: SLINK Operational Scenario Outline

Figure 4-6 shows an assessment of the threats and mission phase priorities for SLINK. The threats are listed in the rows, while our four mission phases are contained in the columns. In each cell are four numbers. The numbers represent judgements about the susceptibility, vulnerability, threat likelihood, and overall rank of the cell with respect to the SLINK's ability to function in the operational environment.

Looking first at the threat likelihood numbers, the microwave threat is considered unlikely. Sabotage is possible or probable, as is HEMP exposure. The other threats are validated and expected. The vulnerability numbers show that the system is most vulnerable to direct physical attack, as indicated by the "3"s in the tactical nuclear and tactical air cells. It is least vulnerable to ECM (as discussed previously). Finally the susceptibility numbers show that the strategic HEMP attack will cover the whole theatre if conducted, and the SLINK is very susceptible (exposed) to HEMP. Since tactical air attacks are pervasive in the theatre, SLINK will most likely be susceptible to those attacks, if it is discovered. SLINK is least susceptible to ESM and ECM, a strong argument for its overall survivability, since the SLINK must be located to be attacked at all.

The circled numbers above the mission phases are judgements about the relative vulnerability of SLINK to the threat during each phase. They are primarily based on exposure time. So, although site preparation is a relatively exposed time period, it is short compared to the time the system spends on the road moving. The most likely time for attack is now judged to be while the system is in place and communicating. The second most likely time is when SLINK is exposed on the road network during a move.

The final numbers are those circled to the right of the threat boxes. These numbers indicate the relative importance of each threat, based on the mission and cell rankings discussed above. As might be expected, the top threats are tactical nuclear and conventional weapons, followed by chemical, ESM, and ECM. The bottom three (HEMP, Sabotage, Microwave) are ranked last mostly because they are considered unlikely by the intelligence agencies.

No threats that were in the initial threat description have been deleted, but some have been downgraded in importance. Note that some threats never made it into the scenario in the first place. These include adversary conventional ground force attacks, direct attacks by adversary ICBMs, or attacks by artillery. These were

MSN PHASE / THREAT	12-72 HRS COMM (1)					1-6 HRS MOVE (2)					30 MIN - 1 HR PREPARE SITE (3)					15 MIN ESTABLISH COMM (4)				
	S	V	T	O	Rank	S	V	T	O	Rank	S	V	T	O	Rank	S	V	T	O	Rank
(1) TACTICAL AIR	2	3	3	0	5	3	3	3	0	1	3	3	3	0	2	2	3	3	0	4
(2) TACTICAL NUCLEAR	3	3	3	0	3	2	3	3	0	9	2	3	3	0	8	2	3	3	0	7
(3) CHEMICAL	2	2	3	0	11	1	1	3	0	14	3	3	3	0	6	2	2	3	0	10
(4) ESM	1	2	3	0	13											1	3	3	0	12
(5) ECM	1	1	3	0	16											1	1	3	0	15
(6) STRATEGIC HEMP	3	2	2	0	20	3	1	2	0	17	3	1	2	0	18	3	3	2	0	19
(7) SABOTAGE	2	3	2	0	24	2	3	2	0	21	2	3	2	0	22	2	3	2	0	23
(8) HI POWER MICROWAVE	3	3	1	0	27						3	2	1	0	25	3	3	1	0	26

1 LOW
2 MED
3 HI

S - SUSCEPTIBILITY
V - VULNERABILITY
T - THREAT LIKELIHOOD

O - OVERALL RANKING

Figure 4-6. SLINK Operational Scenario Refinement never seriously considered because of employment concepts, weapon limitations, and the SLINK system mission and location.

The scenario threats will be eliminated on the basis of consideration of future data as the OT&E progresses, and studies find that, for example, SLINK has such a low noise signal that ESM gear cannot detect it from 100 km away. OT&E might find that the IR signature of the vans was a dead giveaway to orbiting satellites, or that the sabotage threat is the most likely since dedicated teams will be assigned to shadow each peacetime unit. HEMP could be deleted if a consensus of SAC/HQ, AFCSA and NCGS analysts consider it an unlikely threat. Sabotage should be discussed with Army intelligence agencies and the Air Force Security police to better characterize the likelihood and scope of the threat. The analyst should seek intelligence confirmation or dismissal of the HPM satellite threat against a mobile ground target.

We conclude from our operational scenario example that the first four threats to SLINK must be accorded the bulk of OT&E's attention. The key to all threats is the ESM detection of the SLINK, allowing it to be targeted by the adversary with conventional, chemical, or tactical nuclear weapons. More limited studies should be designed to evaluate the ECM and HEMP threats, while more intelligence information is needed to assess the importance of sabotage and the High Power Microwave.

Since no threats were actually deleted in this step, Figure 4-5 still represents the final operational timeline. Of course, Figure 4-6 and the supporting rationale form an integral part of the operational scenario, since it indicates how much attention should be paid to each system/threat interaction. After the analyst has documented the entire thought train presented in this pamphlet, the initial operational scenario is complete.

5.0 INTEGRATION OF SURVIVABILITY IN OT&E

5.1 OVERVIEW

After completing the construction of the operational scenarios, the analyst should take a few moments to reflect on the scenarios, their justifications and the consistency with other elements of the system acquisition process. The scenarios have been developed to give the analyst a basis to focus on OT&E issues in survivability. Do the scenarios appear reasonable to the analyst? Are all major system phases or important functions well represented in time? Are the scenarios logical?

If the analyst feels that the answer to any of these questions is in doubt, what should be done? It seems prudent to complete the test approach and follow-up with some additional information gathering. Perhaps some of the best information sources at this point are the operational commands and the studies groups. The analyst should also consider the broader OT&E program structure and content, and the implications of the operational scenario to the DT&E survivability test program.

5.2 USING COMMANDS AND STUDIES AGENCIES

By discussing the operational survivability scenario with the Air Force studies groups and using commands, corroboration or corrections can be added. For example, AFCSA usually develops force effectiveness studies for programs in the concept development phase, and may already have considered many of the operational scenario factors. SAC, TAC, and other using commands have studies groups that examine the effectiveness of the new system to support fielding the new system. Depending on the system, the analyst may wish to consult with other agencies including:

- Air Force Electronic Warfare Center (AFEWC)
- SURVIAC or DASIAC
- Air Force Electronic Security Command (ESC)
- Air Force Communications Command (AFCC)
- Nuclear Criteria Group Secretariat (NCGS)

The purposes of the studies performed by these groups differ somewhat from OT&E, and may have been performed on the basis of a different intelligence picture. Therefore, the analyst should carefully consider their advice before it is incorporated to prevent performing OT&E on a design or concept instead of the production system.

Operational command personnel are informed sources of not just the concepts of operation for the new systems but the historical perspective of existing systems.

Review of existing scenarios for fielded systems can provide a backdrop for the scenarios the analyst has constructed. Again care must be exercised to assure the scenarios are consistent with the new system philosophy, needs and the evolving threat. Field exercises may also provide a useful set of information to assist the analyst in building the most credible foundation to support his scenarios.

5.3 OTHER SYSTEM OT&E TESTING

After the operational scenarios are constructed and the test approach or plan is written, the analyst is comfortably set -- right? The analyst can be well served by reflecting on the survivability requirement for OT&E and how effectively these can be prosecuted through the integration of the requirements into the broader spectrum of OT&E tests and analysis.

Integration in this sense means to effectively incorporate survivability OT&E requirements with other planned test and analysis efforts. The nonsurvivability objectives in the system OT&E often plan to assess measures or use methods that can address survivability issues. For example, a test to evaluate operator displays of incoming messages may already exist in the OT&E efforts. This test may be an effective tool for examining operator responses to jamming, EMP, and other unplanned system conditions caused by threat effects. The survivability analyst will be able to make use of such tests to the extent that the benign measures reflect survivability parameters and that the methods can be adapted to include threat effects. System level models are also used to answer nonsurvivability objectives, and can sometimes be adapted with minimal effort to incorporate threats.

5.4 JOINT OT&E AND DT&E

Many larger programs (especially strategic and space) are now being conducted as joint DT&E/OT&E efforts. The analyst should also look for potential integration of OT&E survivability requirements into the DT&E efforts. Although this may sound difficult, early identification to the developers of areas of interest will serve the analyst well. The earlier the developer hears about the emerging focus of OT&E, the more receptive he/she is to later inputs. By substantiating OT&E requirements through a well written and comprehensive operational scenario, the analyst can increase the credibility of his requirements with a typically skeptical DT&E community.

For example, there may be a DT&E test to exercise the system C^2 links under threat jammer conditions. If operational personnel, threats, software, messages and equipment are used, the test can satisfy an OT&E data requirement for survivability. Even if the test uses, for example, prototype equipment, proper caveats can often make the data usable by OT&E.

5.5 SUMMARY

This pamphlet described a process that a survivability analyst can use to develop operational scenarios. It uses the term operational scenario to describe the integration of the system mission and critical functions with the most likely threats to the system. The process outlined in this pamphlet differentiates an operational scenario from an intelligence estimate of the threat because the scenario incorporates the system mission and the survivability features of the system.

The process began with describing the system mission objectives, mission timeline, and the critical functions that must be performed during the mission. This step was done first because the mission is, in a sense, the "target" of the threat systems. The mission objective and mission critical functions were important because they define the success criteria for a threat attempting to negate the system.

The threat description was the second step in the process. To write the threat description, the analyst drew heavily on intelligence sources, and supplemented intelligence information with data from the user and the system developer. A list of threat attributes and threat effects was presented to guide the analyst in the content of a threat description.

The final step was to apply the threat description to the mission description and to refine the resulting operational scenario. The refinement process consisted of considering the susceptibility and vulnerability of the system to the threat, and the priority of the mission functions. The factors obtained by these deliberations could aid the analyst in prioritizing the threat/system interactions. The prioritized matrix of threat and system interactions would then form the basis for the amount of effort expended during the OT&E to evaluate the survivability of the system.

REFERENCES

Threat Scenario, Supplement B to B-1B System Level EMP Test Nuclear Assessment Plan, AFOTEC/OASZ, September 1986 (SECRET)

Operational Threat Scenario, Supplement B to MILSTAR Air Force Terminal Nuclear Assessment Plan, AFOTEC/OASS, April, 1987 (SECRET)

APPENDIX A

Index to Air Force Nuclear Survivability Data Base

C^3 SYSTEMS

AACE AIRCRAFT ALERTING COMMUNICATIONS EMP
AASR ADVANCED AIRBORNE SURVEILLANCE RADAR
ABCCC-III AIRBORNE BATTLEFIELD C AND C CAPSULES
ACP AUTOMATIC COMMUNICATIONS PROCESSOR
ADAPTIVE HF/VHF COMMUNICATIONS
AFC2S MODERNIZATION AF COMMAND AND CONTROL SYSTEMS
AF-1 AIR FORCE ONE REPLACEMENT
ASCS ADVANCED SKYWAVE COMMUNICATIONS SYSTEM
ATSR ADVANCED TACTICAL SURVEILLANCE RADAR
ATSS ADVANCED TACTICAL SURVEILLANCE SYSTEM
B-52 ARC-65 (REPLACEMENT HF RADIO)
EC-135
EC-17
E-3A AWACS
E-4B ADVANCED AIRBORNE COMMAND POST (AABNCP)
E-6A
GWEN GROUND WAVE EMERGENCY NET
I-S/A AMPE (INTER-SERV/AGCY AUTO. MESSAGE PROCESSING EXCH.)
JSTARS JOINT SURVEILLANCE & TARGET ATTACK RADAR SYSTEM
JTIDS JOINT TACTICAL DISTRIBUTION SYSTEM
LOGNET AFLC LOGISTICS NETWORKING PROGRAM
MEECN MIN ESSENTIAL EMERGENCY COMMO NETWORK
MEITS MISSION EFFECTIVE INFORMATION TRANSMISSION SYSTEM
NCMC NORAD CHEYENNE MOUNTAIN COMPLEX
PAVE PAWS
PEACEKEEPER ALCC (MX)
SACDIN SAC DIGITAL INFORMATION NETWORK
SCIS SURVIVABLE COMMUNICATIONS INTEGRATION SYSTEM
SCP SECURE CONFERENCING PROJECT
SIS SPACE INTELLIGENCE SYSTEM
SURVIVABLE COMMAND POST
TDF TACTICAL DIGITAL FACILITY
TRI-TAC JOINT TACTICAL COMMUNICATION SYSTEM
WIS WWMCCS INFORMATION SYSTEM
WWABNCP REPLACEMENT

SPACE SYSTEMS

AFSATCOM SCT (DSCS PHASE III)
AFSATCOM SCT (GPS PHASE III)
AFSATCOM SCT (GPS PHASE II)
AFSCN (AF SATELLITE CONTROL NETWORK)
COMPACT SPACE POWER SYSTEMS
DMSP (DEFENSE METEOROLOGICAL SPACE PROGRAM)
DSAT (DEFENSIVE SATELLITE)
DSCS-II (DEFENSE SATELLITE COMMUNICATION SYSTE, PHASE II)
DSCS-III FOLLOW-ON (DEFENSE SATELLITE COMMUNICATIONS SYSTEM)
DSCS-III (DEFENSE SATELLITE COMMUNICATIONS SYSTEM, PHASE III)
DSP FOLLOW-ON (DEFENSE SUPPORT PROGRAM)
DSP - GROUND STATIONS
DSP, SATELLITES 10-13
DSP, SATELLITES 5, 6, 14 AND SUBSEQUENT
FLTSATCOM (FLEET SATELLITE COMMUNICATION SYSTEM)
GPS USER EQUIPMENT (NAVSTAR GLOBAL POSITIONING SYSTEM)
GPS (NAVSTAR GLOBAL POSITIONING SYSTEM)
MILSTAR SATELLITE
MILSTAR TERMINALS
NABS TERMINALS (NATO AIRBASE SATCOM)
NDS (NUCLEAR DETONATION DETECTION SYSTEM)(FORMERLY GPS/IOND)
SATELLITE ATTACK DETECTION SYSTEM
SBSS (SPACE BASED SURVEILLANCE SYSTEM)
SEMWS (SURVIVABLE & ENDURING MISSILE WARNING SYSTEM
SPACE BASED LASER
SPACE BASED RADAR
SPACE SHUTTLE

MISSILE SYSTEMS

ALCM (AIR LAUNCHED CRUISE MISSILES)
AMRAAM (ADVANCED MEDIUM RANGE AIR TO AIR MISSILE)
ASALM
ATCM (ADVANCED TECHNOLOGY CRUISE MISSILE)
B-1 SCAD (AGM-86A)
B-52 SCAD (AGM-86A)
GLCM (GROUND LAUNCHED CRUISE MISSILE)
HOUND DOG II
MINUTEMAN II MISSILE
MINUTEMAN III
MINUTEMAN LCF (LAUNCH CONTROL FACILITY)
MINUTEMAN REENTRY VEHICLE (MK-11C)
MINUTEMAN REENTRY VEHICLE (MK-12A)
MINUTEMAN REENTRY VEHICLE (MK-12)
PEACEKEEPER LAUNCHER/TRANPORTER/OPERATIONAL CONTROL CENTER
PEACEKEEPER MISSILE (MX)
PEACEKEEPER WARHEAD (ABRV) (MK 21)
SICBM HML (MOBILE TRACTOR/TRAILER) (HARD MOBILE LAUNCHER)
SICBM HML (STOPPED * HARDENED) (HARD MOBILE LAUNCHER)
SICBM WCS (SMALL ICBM) (WEAPON CONTROL SYSTEM)
SICBM (SMALL ICBM) (INFLIGHT)
SICBM (SMALL ICBM) (PREFLIGHT)
SRAM-A (AGM-69A)
SRAM-B (AGM-69B)
SRAM-II (XAGM-131A) (FORMERLY AASM)

APPENDIX B

Supplement B (Operational Threat Scenario)

Sample Outline

OPERATIONAL SCENARIO
SUPPLEMENT B to
OT&E XXXXXXX TEST APPROACH/TEST PLAN
TABLE OF CONTENTS

SECTION PAGE

1.0 INTRODUCTION
- 1.1 OVERVIEW
- 1.2 ORGANIZATION OF THE DOCUMENT

2.0 SYSTEM MISSION DESCRIPTION
- 2.1 INTRODUCTION
- 2.2 MISSION ATTRIBUTES
- 2.3 SYSTEM ATTRIBUTES
- 2.4 MISSION DESCRIPTION

3.0 THREAT DESCRIPTION
- 3.1 INTRODUCTION
- 3.2 NUCLEAR THREATS
- 3.3 CONVENTIONAL THREATS
- 3.4 ELECTRONIC WARFARE THREATS
- 3.5 CHEMICAL/BIOLOGICAL THREATS
- 3.6 DIRECTED ENERGY WEAPONS
- 3.7 SUMMARY OF THREATS

4.0 SYSTEM XXXXXX OPERATIONAL SCENARIO
- 4.1 INITIAL APPLICATION
- 4.2 REFINING THE SCENARIO
  - 4.2.1 Susceptibility Analysis
  - 4.2.2 Vulnerability Analysis
  - 4.2.3 Prioritized Mission/Threat Interactions
- 4.3 ADDITIONAL CONSIDERATIONS
- 4.4 SUMMARY OF THE SCENARIO